Administratorhandbuch

BES12

Version 12.2

Veröffentlicht: 2015-08-14
SWD-20150814105910700

Inhalt

Einführung 11

Info zu diesem Handbuch 12

Was ist BES12? 13

Schlüsselmerkmale von BES12 13

Verwendung dieses Handbuchs 15

Schritte zur Verwaltung von BES12 15

Beispiele für die alltäglichen Administrationsszenarien 16

Anmelden bei BES12 18

Info über BES12 Self-Service 19

Verwaltungsoptionen für Android 21

Verwaltungsoptionen für Android-Geräte 22

Informationen zu Android MDM und KNOX MDM 22

Info über Android for Work 24

Info über KNOX Workspace 27

Informationen zu Secure Work Space für Android-Geräte 30

Administratoren 33

Einrichten von Administratoren 34

Schritte zum Einrichten von Administratoren 34

So wählt BES12 die zuzuweisende Rolle aus 34

Erstellen und Verwalten von Administratorgruppen 35

Erstellen und Verwalten von Administratoren 36

Verwalten von Rollen 38

Secure Work Space 51

Einrichten von Secure Work Space für iOS- und Android-Geräte 52

Enterprise-Konnektivität und Proxy-Server 52

Verwalten von Geräten mit einem geschäftlichen Bereich 53

Aktualisieren von Apps für den geschäftlichen Bereich 54

Testen der Secure Work Space-Verbindung 54

Erneutes Erstellen der Secure Work Space-Verbindung 54

Profile und Variablen 57

Verwenden von Profilen....58
Zuweisen von Profilen....58
So wählt BES12 die zuzuweisenden Profile aus....59
Verwalten von Profilen....61
Zuweisen eines Rangs zu Profilen....61
Anzeigen eines Profils....61
Ändern der Profileinstellungen....62
Entfernen eines Profils aus Benutzerkonten oder Benutzergruppen....62
Löschen eines Profils....63
Verwenden von Variablen....64
Verwenden von Variablen in Profilen....64
Standardvariablen....64
Benutzerdefinierte Variablen....66
Zertifikate....69
Verwalten von Zertifikaten mithilfe von Profilen....70
Senden von Zertifikaten an Geräte....71
Erstellen von Profilen mit Zertifizierungsstellenzertifikat....71
Erstellen von SCEP-Profilen....73
Erstellen von Profilen für freigegebene Zertifikate....74
Integration von BES12 mit der Entrust-Software Ihrer Organisation....76
Schritte zur Integration von BES12 mit der Entrust-Software Ihrer Organisation....76
Hinzufügen einer Verbindung zur Entrust-Software Ihrer Organisation....77
Senden der Entrust-Zertifizierungsstellenzertifikate an Geräte....77
Bereitstellung von Entrust-Client-Zertifikaten an Geräte....78
Geschäftsverbindungen....81
Geschäftsverbindungen für Geräte einrichten....82
Schritte zum Einrichten von Geschäftsverbindungen für Geräte....82
Verwalten von geschäftlichen Verbindungen mithilfe von Profilen....82
Bewährtes Verfahren: Erstellen von Profilen für Geschäftsverbindungen....84
Einrichten des geschäftlichen E-Mail-Kontos für Geräte....84
Einrichten von Proxy-Konfigurationen für Geräte....94
Einrichten von geschäftlichen Wi-Fi-Netzwerken für Geräte....97
Einrichten von geschäftlichen VPNs für Geräte....98
Einrichten von Enterprise-Konnektivität für Geräte....102
Einrichten einer Authentifizierung bei einmaliger Anmeldung für Geräte....103
Verwenden von BlackBerry Secure Connect Plus für sichere Verbindungen mit geschäftlichen Ressourcen....107

Schritte zum Aktivieren von BlackBerry Secure Connect Plus 107
Anforderungen an Server und Geräte..... 108
Datenfluss bei der Erstellung eines sicheren IP-Tunnels durch BlackBerry Secure Connect Plus 109
Lastverteilung und hohe Verfügbarkeit für BlackBerry Secure Connect Plus 110
Aktivieren und Konfigurieren von BlackBerry Secure Connect Plus 110
Fehlerbehebung bei BlackBerry Secure Connect Plus..... 113

Gerätestandards..... 117

Einrichten der Gerätestandards für Ihre Organisation..... 118
Schritte zum Einrichten der Gerätestandards für Ihre Organisation..... 118
Verwalten der Standards Ihrer Organisation mit Profilen..... 118
Durchsetzen von Kompatibilitätsregeln für Geräte..... 119
Filtern von Webinhalten auf iOS-Geräten..... 122
Begrenzung von Geräten auf eine einzelne App..... 124
Steuern der Softwareversionen, die Benutzer auf BlackBerry 10-Geräten installieren können..... 126
Verwalten von E-Mail- und Webdomänen für iOS 8-Geräte..... 128
Konfigurieren von zugelassenen und gesperrten Domänen auf Geräten mit einem geschäftlichen Bereich..... 129
Erstellen von Organisationshinweisen zur Anzeige auf BlackBerry 10-Geräten..... 130
Anzeigen von Organisationsinformationen auf Geräten 131
Erstellen von Websymbolen für iOS-Geräte..... 133
Einrichten der Standortbestimmung für iOS-Geräte..... 134

IT-Richtlinien..... 137

Steuern von Gerätefunktionen mithilfe von IT-Richtlinien..... 138
Schritte zum Verwalten von IT-Richtlinien..... 138
Einschränken und Zulassen von Gerätefunktionen..... 139
So wählt BES12 die zuzuweisenden IT-Richtlinien aus..... 139
Erstellen und Verwalten von IT-Richtlinien..... 140
Steuern von BlackBerry OS-Gerätefunktionen mithilfe von IT-Richtlinien..... 144
Schritte zum Verwalten von BlackBerry OS-IT-Richtlinien..... 144
Einschränken und Zulassen von BlackBerry OS-Gerätefunktionen..... 145
Vorkonfigurierte BlackBerry OS-IT-Richtlinien..... 145
Zuweisen von BlackBerry OS-IT-Richtlinien und Auflösen von Konflikten zwischen IT-Richtlinien..... 146
Deaktivieren von BlackBerry OS-Geräten, auf die keine IT-Richtlinien angewendet wurden..... 148
Erstellen und Verwalten von BlackBerry OS IT-Richtlinien..... 149

Apps..... 151

Verwalten von Apps auf Geräten..... 152
Schritte zum Verwalten von Apps..... 152

Hinzufügen und Löschen von Apps aus der Liste der verfügbaren Apps..... 152
Verhindern, dass Benutzer bestimmte iOS-, Android- und Windows Phone-Apps installieren.....169
Verwalten von App-Gruppen..... 171
Verwalten von Apple VPP-Konten..... 173
Ändern, ob die App erforderlich oder optional ist..... 174
Anzeigen des Status von Benutzerkonten zugewiesenen Apps und App-Gruppen..... 175
Anzeigen, welche Apps Benutzergruppen zugewiesen wurden..... 175
Aktualisieren der Daten in der Liste der verfügbaren Apps..... 175
Aktualisieren von App-Berechtigungen für Android for Work-Apps.....176
Festlegen des Organisationsnamens für BlackBerry World 176
Verwalten von Apps auf BlackBerry OS-Geräten..... 178
Vorbereiten der Verteilung von BlackBerry Java Applications 178
Konfigurieren von Anwendungssteuerungsrichtlinien..... 180
Anwendungssteuerungsrichtlinien für nicht aufgeführte Anwendungen..... 183
Erstellen von Softwarekonfigurationen..... 185
Installieren von BlackBerry Java Applications auf einem BlackBerry OS-Gerät über einen zentralen Computer.....187
Anzeigen der Benutzer, die eine BlackBerry Java Application auf ihren BlackBerry OS-Geräten installiert haben..... 188
Synchronisierungsregeln für miteinander in Konflikt stehende Einstellungen in Softwarekonfigurationen.....189

Benutzer und Geräte..... 197

Verwalten von Benutzergruppen und Benutzerkonten..... 198
Schritte zur Erstellung von Benutzergruppen und Benutzerkonten.....198
Erstellen und Verwalten von Benutzergruppen..... 199
Erstellen und Verwalten von Benutzerkonten.....210
Verwenden von Filtern zum Anpassen der Benutzer- und Geräteansicht 225
Verwalten von Gerätegruppen..... 227
Schritte zum Erstellen und Verwalten von Gerätegruppen.....227
Erstellen einer Gerätegruppe..... 227
Anzeigen einer Gerätegruppe..... 230
Klicken Sie auf den Namen einer Gerätegruppe..... 231
Löschen einer Gerätegruppe.....231
Aktivieren von beim DEP registrierten iOS-Geräten.....232
Voraussetzung: Verwendung des BES12 Client für beim DEP registrierte Geräte..... 232
Schritte zum Aktivieren von Geräten, die beim DEP registriert sind..... 232
Registrieren von iOS-Geräten beim DEP und Zuweisen eines MDM-Servers..... 233
Zuweisen von Registrierungskonfigurationen zu iOS-Geräten.....233
Entfernen einer iOS-Geräten zugewiesenen Registrierungskonfiguration..... 234
Verwalten von Registrierungskonfigurationen..... 234

Anzeigen der Einstellungen einer zugewiesenen Registrierungskonfiguration....236
Anzeigen der Benutzerdetails für ein aktiviertes Gerät....236
Aktivieren von Geräten....237
Schritte zur Aktivierung von Geräten....237
Voraussetzungen: Aktivierung....238
Lizenzanforderungen für Aktivierungsarten....238
Verwalten des Standardablaufs und der Länge des Aktivierungskennworts....242
Abschalten der Benutzerregistrierung bei der BlackBerry Infrastructure....243
Unterstützen von Android for Work-Aktivierungen....243
Verwalten von Vorlagen für die Aktivierungs-E-Mail....245
Steuern der Geräteaktivierungseinstellungen mithilfe von Aktivierungsprofilen....247
Einrichten eines Aktivierungskennworts und Senden einer Aktivierungs-E-Mail-Nachricht....253
Zulassen, dass Benutzer Aktivierungskennwörter festlegen....254
Aktivieren eines BlackBerry 10-Geräts....254
Aktivieren eines BlackBerry OS-Geräts....255
Aktivieren eines iOS-Geräts....256
Aktivieren eines Android-Geräts....256
Aktivieren eines Windows Phone-Geräts....257
Aktivieren von BlackBerry 10-Geräten mithilfe von BlackBerry Wired Activation Tool....258
Tipps zur Fehlersuche bei der Geräteaktivierung....261
Verwalten von Geräten....266
Verwenden von Dashboard-Berichten....266
Verwenden von IT-Administrationsbefehlen zum Verwalten von Geräten....267
Anzeigen und Speichern eines Geräteberichts....276
Überprüfen, ob ein Gerät für den Zugriff auf geschäftliche E-Mails und Terminplanerdaten zugelassen ist....277
Exchange Gatekeeping....278
Deaktivieren von Geräten....279
Bestimmen des Standorts von iOS-Geräten....279
Wartung und Überwachung....281
Verwendung von Protokolldateien....282
Verwalten von BES12-Protokolldateien....282
Auffinden der Protokolldateien....285
Lesen der Protokolldateien....286
Überwachen der App-Aktivität auf BlackBerry 10- und BlackBerry OS-Geräten....292
Anzeigen der Geräteaktionen....293
Auslesen von Protokolldateien aus Geräten....294
Überwachungsaktionen in BES12....296

Konfigurieren von Überwachungseinstellungen....296
Anzeigen und Filtern des Überwachungsprotokolls....297
Exportieren des Überwachungsprotokolls in eine .csv-Datei....297
Löschen alter Überwachungsdatensätze....297
Verwenden von SNMP zur Überwachung von BES12....299
SNMP-Zähler für Enterprise-Konnektivität....299
SNMP-Zähler für BES12 Core....322
SNMP-Zähler für BlackBerry Secure Connect Plus....326
Profileinstellungen....329
E-Mail-Profileinstellungen....330
Allgemein: E-Mail-Profileinstellungen....330
BlackBerry 10: E-Mail-Profileinstellungen....331
iOS: E-Mail-Profileinstellungen....342
Android: E-Mail-Profileinstellungen....346
Windows Phone: E-Mail-Profileinstellungen....349
IMAP/POP3-E-Mail-Profileinstellungen....351
Allgemein: IMAP/POP3-E-Mail-Profileinstellungen....351
iOS: IMAP/POP3-E-Mail-Profileinstellungen....352
Android: IMAP/POP3-E-Mail-Profileinstellungen....353
Windows Phone: IMAP/POP3-E-Mail-Profileinstellungen....354
SCEP-Profileinstellungen....355
Allgemein: SCEP-Profileinstellungen....355
BlackBerry 10: SCEP-Profileinstellungen....357
iOS: SCEP-Profileinstellungen....361
Android: SCEP-Profileinstellungen....364
Wi-Fi-Profileinstellungen....369
Allgemein: Wi-Fi-Profileinstellungen....369
BlackBerry 10: Wi-Fi-Profileinstellungen....369
iOS: Wi-Fi-Profileinstellungen....375
Android: Wi-Fi-Profileinstellungen....381
Windows Phone: Wi-Fi-Profileinstellungen....386
VPN-Profileinstellungen....391
BlackBerry 10: VPN-Profileinstellungen....391
iOS: VPN-Profileinstellungen....404
Android: VPN-Profileinstellungen....409
Unterstützte Leistungsmerkmale nach Gerätetyp....415

Unterstützte Leistungsmerkmale nach Gerätetyp..... 416
Richtlinien-Referenztabelle..... 423
Produktdokumentation..... 425
Glossar..... 427
Rechtliche Hinweise..... 431

Einführung

Erfahren Sie mehr über BES12 und die Verwendung dieses Handbuchs.

Info zu diesem Handbuch

1

BES12 unterstützt Sie bei der Verwaltung der Geräte in Ihrer Organisation. Dieses Handbuch beschreibt die Verwaltung von BES12 von der Erstellung von Administratoren über die Einrichtung der Gerätebenutzer bis hin zur Wartung und Überwachung von BES12.

Es ist für erfahrene und neue IT-Mitarbeiter gedacht, die für die Einrichtung und Verwaltung von BES12 verantwortlich sind. Bevor Sie dieses Handbuch verwenden, sollte die BES12-Umgebung wie im *Konfigurationshandbuch* zu BES12 beschrieben von einem erfahrenen IT-Mitarbeiter konfiguriert werden.

Was ist BES12?

2

BES12 ist eine EMM-Lösung von BlackBerry. EMM-Lösungen unterstützen Sie bei folgenden Aufgaben:

- Verwalten von Mobilgeräten Ihres Unternehmens zum Schutz von geschäftlichen Daten
- Verbindung mobiler Mitarbeiter mit den benötigten Informationen
- Bereitstellung von effizienten Geschäftstools für Administratoren

Mit BES12 können Sie folgende Gerätetypen verwalten:

- BlackBerry 10
- BlackBerry OS (Version 5.0 bis 7.1)
- iOS
- Android (einschließlich Samsung KNOX)
- Windows Phone

Diese Geräte können über eine einzelne, vereinfache Benutzerschnittstelle mit branchenführender Sicherheit verwaltet werden.

Schlüsselmerkmale von BES12

Funktion	Beschreibung
Verwaltung zahlreicher Gerätetypen	Sie können Geräte der Plattformen BlackBerry 10, BlackBerry OS (Version 5.0 bis 7.1), iOS, Android und Windows Phone verwalten.
Eine einheitliche Benutzeroberfläche	Sie können alle Geräte an einem Ort anzeigen und über eine einzige webbasierte Benutzeroberfläche auf alle Verwaltungsaufgaben zugreifen. Sie können Verwaltungsaufgaben gemeinsam mit anderen Administratoren erledigen, die gleichzeitig auf die Verwaltungskonsole zugreifen können.
Bewährtes, sicheres Benutzererlebnis	Die Gerätesteuerungen ermöglichen eine präzise Verwaltung der Verbindung von Geräten mit dem Netzwerk, der aktivierten Leistungsmerkmale und der verfügbaren Apps. Ob die Geräte nun Eigentum Ihres Unternehmens oder Ihrer Benutzer sind, Sie können in jedem Fall die Daten Ihres Unternehmens schützen.
Vereinbarkeit von geschäftlichen und persönlichen Anforderungen	Die Technologien von BlackBerry Balance und Secure Work Space zielen darauf ab, dass persönliche und geschäftliche Informationen auf den Geräten separat und sicher gehalten werden. Wenn das Gerät verloren geht oder der

Funktion	Beschreibung
	Mitarbeiter das Unternehmen verlässt, können Sie entweder nur die geschäftlichen Informationen oder aber alle Informationen vom Gerät löschen.
BlackBerry Secure Connect Plus	BlackBerry Secure Connect Plus ist eine BES12-Komponente, die einen sicheren IP-Tunnel zwischen Apps für den geschäftlichen Bereich auf BlackBerry 10-, KNOX Workspace- und Android for Work-Geräten und dem Netzwerk des Unternehmens herstellt. Dieser Tunnel ermöglicht Benutzern den Zugriff auf Ressourcen hinter der Firewall des Unternehmens und stellt zugleich die Sicherheit von Daten mithilfe von Standardprotokollen und durchgängiger Verschlüsselung sicher. Unterstützte Geräte verwenden BlackBerry Secure Connect Plus, wenn die Geräte nicht auf das geschäftliche Wi-Fi-Netzwerk oder VPN zugreifen können (wenn sich der Benutzer z. B. nicht vor Ort und nicht im Bereich des geschäftlichen Wi-Fi-Netzwerks befindet).

Verwendung dieses Handbuchs

3

Die Aufgaben in diesem Handbuch sind in einer bestimmten Reihenfolge dargestellt, damit Sie schon nach kurzer Zeit und auf die effektivste Art und Weise Ihren Verwaltungsaufgaben nachgehen können, insbesondere wenn die Verwaltung von BES12 für Sie Neuland ist.

Sie müssen möglicherweise nicht alle Aufgaben ausführen. Sie können sich dazu entscheiden, nur bestimmte Gerätetypen zu aktivieren, geschäftliche und private Daten auf unterschiedliche Weise zu trennen oder verschiedene Kompatibilitätsregeln, Gerätefunktionen und Verbindungen zu erzwingen.

Schritte zur Verwaltung von BES12

Zur Verwaltung von BES12 führen Sie die folgenden Aktionen aus:

Schritt	Aktion
1	Wenn Sie Verwaltungsaufgaben mit anderen IT-Mitarbeitern teilen möchten, richten Sie Administratoren ein.
2	Richten Sie die geschäftlichen Verbindungen ein (zum Beispiel E-Mail, Wi-Fi und VPN).
3	Richten Sie die Gerätestandards ein (zum Beispiel Kompatibilitätsregeln).
4	Aktualisieren Sie die Standard-IT-Richtlinie, oder erstellen Sie neue IT-Richtlinien.
5	Legen Sie fest, welche Apps an die Geräte gesendet werden.
6	Legen Sie Benutzer und Gruppen an.
7	Weisen Sie den Benutzern und Gruppen Geschäftsverbindungen, Gerätestandards, IT-Richtlinien und Apps zu.
8	Unterstützen Sie die Benutzer bei der Aktivierung ihrer Geräte.
9	Warten und überwachen Sie BES12.

Beispiele für die alltäglichen Administrationsszenarien

Die folgenden Szenarien sind Beispiele für unterschiedliche Optionen, die Sie bei der Einrichtung verschiedener Geräte für unterschiedliche Benutzer wählen können.

Szenario	Mögliche Aufgaben
BlackBerry 10-Geräte für die geschäftliche und persönliche Verwendung verwalten	• Profile für Zertifikate erstellen • Ein Profil für die einmalige Anmeldung zur Sicherung von Geschäftsdomänen erstellen • Ein Profil für einen Proxy-Server erstellen • Die Aktivierungsart „Geschäftlich und persönlich – Unternehmen“ oder „Geschäftlich und persönlich – Reguliert“ auswählen
Die grundlegende Geräteverwaltung von iOS-, Android- oder Windows Phone-Geräten anwenden	• Profile für geschäftliche E-Mails und geschäftliches Wi-Fi erstellen • Die Standard-IT-Richtlinie ändern, um ein Gerätekennwort zu erzwingen • Eine geschäftliche App auswählen, um sie an das Gerät zu senden • Die Aktivierungsart „MDM-Steuerelemente“ auswählen
Geräte mit BlackBerry OS (Version 5.0 bis 7.1) verwalten	• Die Standard-IT-Richtlinie im BlackBerry OS ändern, um ein Gerätekennwort zu erzwingen • Die IT-Richtlinie im BlackBerry OS erneut an die Geräte senden
iOS- oder Android-Geräte mit einer zusätzlichen Sicherheit für geschäftliche Daten einrichten	• Profil für die Enterprise-Konnektivität erstellen, um Datenübertragungen zusätzlich zu schützen • S/MIME für zusätzliche E-Mail-Sicherheit aktivieren • Kompatibilitätsprofil erstellen, um bei einem entsperrten oder gehackten Gerät den Zugriff auf geschäftliche Ressourcen zu verhindern • Ein Webinhaltsfilter-Profil erstellen, um die Websites einzuschränken, die ein Gerätebenutzer aufrufen kann. • Secure Work Space einrichten, um geschäftliche Daten zu trennen und zu sichern • Eine App sichern, um sie an das Gerät zu senden
BlackBerry 10-Geräte nur für die geschäftliche Verwendung einrichten	• Profile für Zertifikate und VPN erstellen

Szenario	Mögliche Aufgaben
	• S/MIME für zusätzliche E-Mail-Sicherheit aktivieren • IT-Richtlinie erstellen, um die Verwendung der Gerätekamera zu verhindern • Wählen Sie die Aktivierungsart „Nur geschäftlicher Bereich“ aus
Richten Sie ein iOS-Gerät ein, das für Softwaredemos auf eine App begrenzt ist	• Erstellen eines Profils für den App-Sperrmodus

Anmelden bei BES12

4

Die Verwaltungskonsole ermöglicht das Ausführen administrativer Aufgaben für Geräte in Ihrer Organisation, die von BES12 verwaltet werden.

Bevor Sie beginnen:

- Suchen Sie die Webadresse (z. B. https://<*hostname*>/admin/index.jsp?tenant=<*tenant*>) und die Anmeldeinformationen für die Verwaltungskonsole. Sie finden die Informationen im Posteingang des E-Mail-Kontos, das mit Ihrem BES12-Konto verknüpft ist.
- Die Authentifizierungsmethode und die Domäne müssen Ihnen bekannt sein (gilt nur für Microsoft Active Directory-Authentifizierung).

1. Geben Sie im Browser die Webadresse für die BES12-Verwaltungskonsole Ihrer Organisation ein.
2. Geben Sie im Feld **Benutzername** Ihren Benutzernamen ein.
3. Geben Sie im Feld **Kennwort** Ihr Kennwort ein.
4. Führen Sie in der Dropdown-Liste **Anmelden mit** ggf. eine der folgenden Aktionen aus:
    - Klicken Sie auf **Direkte Authentifizierung**.
    - Klicken Sie auf **LDAP-Authentifizierung**.
    - Klicken Sie auf **Microsoft Active Directory-Authentifizierung**. Geben Sie im Feld **Domäne** die Microsoft Active Directory-Domäne ein.
5. Klicken Sie auf **Anmelden**.

Wenn Sie fertig sind: Sie können Ihr Anmeldekennwort ändern, indem Sie auf das Benutzersymbol oben rechts in der Verwaltungskonsole klicken.

Info über BES12 Self-Service

5

BES12 Self-Service ist eine Webanwendung, die Sie den Benutzern zur Verfügung stellen können, damit diese bestimmte Vorgänge durchführen können, beispielsweise Kennwörter erstellen, Geräte sperren oder Daten von den Geräten löschen. Eine Installation von Software auf den Geräten der Benutzer ist für die Verwendung von BES12 Self-Service nicht erforderlich.

Sie müssen den Benutzern die BES12 Self-Service-Anmeldedaten zur Verfügung stellen. Diese Daten können Sie entweder per E-Mail senden oder die E-Mail-Vorlage für die Aktivierung so ändern, dass sie die Daten enthält. Sie können die Benutzer ebenfalls zwingen, eine Mitteilung zu lesen und anzunehmen, bevor sie sich bei BES12 Self-Service anmelden können. Weitere Informationen finden Sie unter „Anzeigen einer Anmeldemitteilung“. Folgende Informationen sind erforderlich:

- Webadresse: Die Webadresse für BES12 Self-Service wird auf der Verwaltungskonsole unter „Einstellungen > Self-Service“ angezeigt.
- Benutzername und Kennwort: Unternehmensverzeichnisbenutzer können sich mit ihren Unternehmensbenutzernamen und -kennwörtern anmelden. Für lokale Benutzer müssen Sie die Benutzernamen und temporären Kennwörter erstellen.
- Domänenname: Microsoft Active Directory-Benutzer benötigen den Domänennamen.

Verwaltungsoptionen für Android

Erfahren Sie mehr über die Optionen zur Verwaltung von Android-Geräten.

Multiplatform

Verwaltungsoptionen für Android-Geräte 6

BES12 umfasst verschiedene Optionen zum Aktivieren und Verwalten von Android-Geräten. Die gewählten Optionen hängen von der Art der verwalteten Android-Geräte und den Sicherheitsanforderungen des Unternehmens ab.

BES12 unterstützt die folgenden Verwaltungsoptionen.

Verwaltungsoption	Beschreibung
Android MDM und KNOX MDM	Diese Option bietet einfach Steuerelemente zur Verwaltung aller Android-Geräte.
Android for Work	Diese Option erstellt eine separates geschäftliches Profil auf Android-Geräten.
KNOX Workspace	Diese Option erstellt einen verschlüsselten KNOX Workspace auf Samsung-Geräten.
Secure Work Space	Diese Option erstellt einen verschlüsselten geschäftlichen Bereich auf Android-Geräten. (Secure Work Space wird auch auf iOS-Geräten unterstützt.)

Unabhängig von gewählten Verwaltungsoption stehen Ihnen folgende BES12-Merkmale zur Verfügung:

- Sichere Verbindung für Verwaltungsdaten von BES12 über die BlackBerry Infrastructure mit BES12 Client auf den Geräten
- Integration in das Verzeichnis des Unternehmens zur Synchronisierung von Benutzerdaten
- Webbasierte Verwaltungskonsolen Administratoren und Benutzer

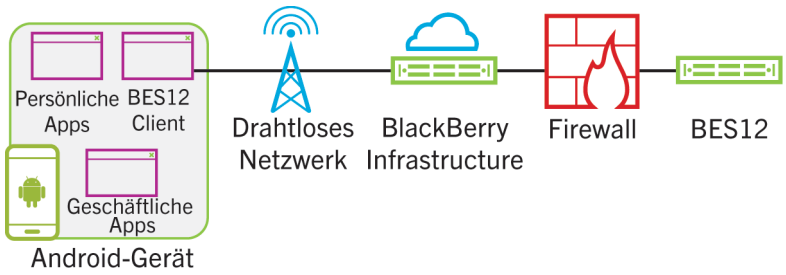
Informationen zu Android MDM und KNOX MDM

Android MDM verwendet die einfachen Android OS-eigenen Verwaltungsoptionen zur Geräteverwaltung. Es wird kein separater geschützten Container für Apps und Daten erstellt.

KNOX MDM ähnelt Android MDM, steht aber nur für Samsung-Geräte zur Verfügung. KNOX MDM bietet erweiterte Funktionen und einen größeren Satz IT-Richtlinienregeln. BES12 aktiviert automatisch Samsung-Geräte zur Verwendung von KNOX MDM, sofern die Geräte es unterstützen.

Zur Verwendung von Android MDM und KNOX MDM aktivieren Sie Geräte mit der Aktivierungsart MDM-Steuerelemente. MDM-Steuerelemente erfordert eine Silver-Lizenz. Weitere Informationen zu Lizenzen finden Sie in der Dokumentation zur Lizenzierung.

Architektur: Android MDM und KNOX MDM



Komponente	Beschreibung
Android-Geräte	Android-Geräte werden in BES12 zur Verwendung der Funktionen von Android MDM bzw. KNOX MDM aktiviert. KNOX MDM wird nur auf Samsung-Geräten unterstützt.
BES12 Client	Der BES12 Client stellt eine Verbindung mit BES12 her, um Verwaltungsbefehle zu empfangen.
Geschäftliche Apps	Geschäftliche Apps sind solche, die Sie als erforderlich oder optional festlegen.
BlackBerry Infrastructure	Die BlackBerry Infrastructure registriert Benutzerinformationen zur Aktivierung und Verwaltung von Geräten. Alle zwischen der BlackBerry Infrastructure und BES12 ausgetauschten Daten werden authentifiziert und mit AES-256 verschlüsselt.
BES12	BES12 ist die EMM-Lösung von BlackBerry, mit der Sie Android-Geräte verwalten können.

Verwaltungsfunktionen für Android MDM- KNOX MDM-Geräte

In der folgenden Tabelle werden die Funktionen zur Verwaltung von Geräten, die Android MDM oder KNOX MDM verwenden, erläutert:

Funktion	Beschreibung
IT-Richtlinienverwaltung	BES12 unterstützt eine Reihe von IT-Richtlinienregeln zur Steuerung von Android-Geräten. Mit IT-Richtlinienregeln können Sie Geräte verschlüsseln, Kennwortanforderungen festlegen und die Kamera deaktivieren. Wenn Sie ein Gerät zur Verwendung von KNOX MDM aktivieren, können Sie einen erweiterten Satz IT-Richtlinien, Browsereinstellungen und Konnektivitätsoptionen konfigurieren.
Wi-Fi und VPN-Profile	BES12 unterstützt Wi-Fi-Profile, mit deren Hilfe Sie Verbindungen mit dem Unternehmensnetzwerk konfigurieren können. VPN-Profile werden in Kombination mit diesen Verwaltungsoptionen nicht unterstützt.

Funktion	Beschreibung
E-Mail	Sie können ein E-Mail-Profil konfigurieren, durch das automatisch eine Exchange ActiveSync-, IMAP- oder POP3-Verbindung mit der geschäftlichen E-Mail und dem Kalender eingerichtet wird. KNOX MDM unterstützt nur Exchange ActiveSync.
App-Verwaltung	Sie können geschäftliche Apps auf Android-Geräten installieren, entfernen und aktualisieren. Sie können auch eine Liste zulässiger und gesperrter Apps verwalten.
Kompatibilität	Sie können die Aktionen konfigurieren, die ausgeführt sollen, wenn ein Gerät gerootet wird. Sie können Richtlinientreue für erforderliche Apps durchsetzen. Wenn Sie Android MDM-Geräte aktivieren, können außerdem Richtlinientreueregeln für gesperrte Apps einrichten. Wenn Sie KNOX MDM-Geräte aktivieren, können Sie eine Liste gesperrter Apps konfigurieren, die vom BES12 Client automatisch entfernt werden, wenn sie vorhanden sind, bzw. deren Installation er verhindert.
App-Sperrmodus	Wenn Sie KNOX MDM-Geräte aktivieren, können Sie ein Profil konfigurieren, mit dem Geräte auf die Ausführung einer oder mehrerer Apps zu Schulungszwecken oder Verkaufsvorführungen beschränkt werden. Sie können die Apps angeben, die auf den Geräten ausgeführt werden sollen.

Info über Android for Work

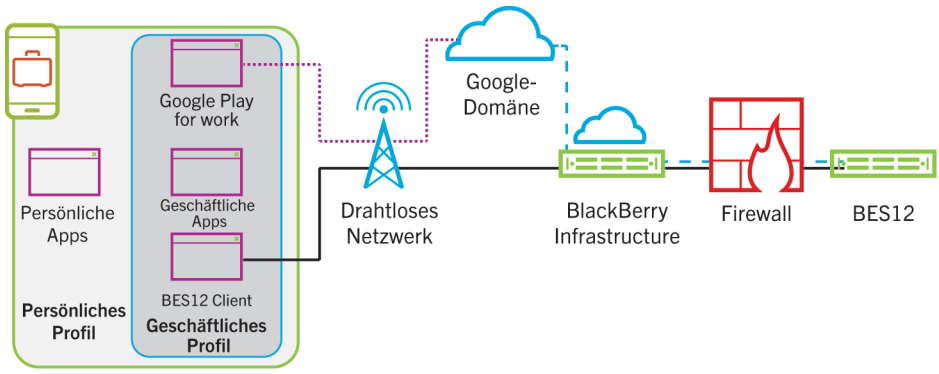
Android for Work ist eine von Google entwickelte Funktion, die zusätzliche Sicherheit für Unternehmen bietet, die Android-Geräte verwalten und die Verwendung ihrer Daten und Apps auf Android-Geräten zulassen möchten. Es bietet Funktionen zur Vereinheitlichung geschäftlicher und persönlicher Anforderungen auf Android-Geräten, die nicht dem Unternehmen gehören. Sie können mit Android for Work beispielsweise geschäftliche E-Mail auf privaten Geräten so einrichten, dass Ihre Inhalte dennoch sicher sind.

Android for Work erfordert, dass im Unternehmen eine Google-Domäne eingerichtet ist und die Benutzer ein Google-Konto für geschäftliche E-Mail haben. Es lässt sich in Google Play zur Verwaltung geschäftlicher Apps im geschäftlichen Profil integrieren.

Zur Verwendung von Android for Work aktivieren Sie Geräte mit der Aktivierungsart „Geschäftlich und persönlich – Benutzer-Datenschutz (Android for Work)“ oder „Geschäftlich und persönlich – Benutzer-Datenschutz (Android for Work - Premium)“. Geschäftlich und persönlich – Benutzer-Datenschutz (Android for Work)-Aktivierungen erfordern eine Silver-Lizenz. Geschäftlich und persönlich – Benutzer-Datenschutz (Android for Work - Premium)-Aktivierungen erfordern eine Gold-Lizenz. Wenn Sie BlackBerry Secure Connect Plus verwenden möchten, müssen Sie die Aktivierungsart „Geschäftlich und persönlich – Benutzer-Datenschutz (Android for Work - Premium)“ verwenden.

Weitere Informationen zu Lizenzen finden Sie in der Dokumentation zur Lizenzierung. Weitere Informationen zu Android for Work finden Sie unter https://www.android.com/work/.

Architektur: Android for Work



Android for Work-Gerät

Komponente	Beschreibung
Android for Work-Geräte	Android for Work-Geräte sind Android-Geräte, die in BES12 aktiviert sind und Android for Work verwenden.
Persönliches Profil	Das persönliche Profil enthält die persönlichen Apps sowie die Android-Plattform und -Dienste (z. B. die Zwischenablagen-App). Wenn Sie ein Gerät mit der Aktivierungsart „Geschäftlich und persönlich – vollständige Kontrolle (Android for Work)“ aktivieren, können Sie Aspekte des persönlichen Profils mithilfe von IT-Richtlinienregeln verwalten.
Geschäftliches Profil	Das geschäftliche Profil wird erstellt, wenn Sie ein Gerät in BES12 mit einer Android for Work-Aktivierungsart aktivieren. Es enthält die folgenden Apps: • BES12 Client, der eine Verbindung mit BES12 für den Empfang von Verwaltungsbefehlen herstellt • Google Play for Work, das eine Verbindung mit der Google-Domäne des Unternehmens zum Herunterladen und Installieren geschäftlicher Apps herstellt • Geschäftliche Apps, die eine Verbindung mit dem Unternehmensnetzwerk für den Zugriff auf Daten herstellen Wenn eine App sowohl im persönlichen als auch im geschäftlichen Profil ausgeführt werden kann (z. B. Google Chrome), wird eine separate Instanz der App in das geschäftliche Profil kopiert.
Google-Domäne	Die Google-Domäne des Unternehmens ermöglicht die Verwaltung von Benutzern und geschäftlichen Apps. Es gibt zwei Arten von Google-Domänen: • Verwaltete Google-Domäne, wenn Google für E-Mail, Kalender usw. genutzt wird • Google Apps-Domäne, wenn eine andere E-Mail-Lösung (z. B.Microsoft Exchange) verwendet und Google-Konten nur zur Verwaltung von Android for Work-Geräten benötigt werden

Komponente	Beschreibung
BlackBerry Infrastructure	In der BlackBerry Infrastructure werden Benutzerinformationen für die Geräteaktivierung registriert. Sie bietet zudem eine Verbindung mit der Google-Domäne, damit BES12 auf das Google-Verzeichnis des Unternehmens und Google Play for Work zugreifen kann. Alle zwischen der BlackBerry Infrastructure und BES12 ausgetauschten Daten werden authentifiziert und mit AES-256 verschlüsselt.
BES12	BES12 ist die EMM-Lösung von BlackBerry, mit der Sie Android for Work-Geräte verwalten können.

Sicherheits- und Verwaltungsfunktionen für Android for Work-Geräte

In der folgenden Tabelle werden die Verwaltungsfunktionen erläutert, die Sie bei Aktivierung von Geräten zur Verwendung von Android for Work nutzen können:

Funktion	Beschreibung
IT-Richtlinienverwaltung	BES12 unterstützt eine Reihe von IT-Richtlinienregeln zur Steuerung von Android for Work-Geräten. Mit IT-Richtlinienregeln können Sie Geräte Kennwortanforderungen konfigurieren und die Kamera deaktivieren.
Wi-Fi	BES12 unterstützt Wi-Fi-Profile, mit deren Hilfe Sie Verbindungen mit dem Unternehmensnetzwerk konfigurieren können. Android for Work-Geräte unterstützen VPN-Profile nicht.
E-Mail	Sie können ein E-Mail-Profil konfigurieren, durch das eine Exchange ActiveSync-Verbindung mit der geschäftlichen E-Mail und dem Kalender eingerichtet wird.
App-Verwaltung	Sie können geschäftliche Apps auf Android for Work-Geräten installieren, entfernen und aktualisieren. Apps müssen im Google Play for Work-Store des Unternehmens zur Verfügung stehen. Sie können auch eine Liste zulässiger und gesperrter Apps verwalten.
App-Konfiguration	Basierend auf den Einstellungen der geschäftlichen Apps können Sie Einschränkungen für geschäftliche Apps konfigurieren, denen diese genügen müssen. Beispielsweise können Sie mithilfe von BES12 verhindern, dass die Google Chrome-App im geschäftlichen Profil im Inkognitomodus ausgeführt wird.
Kompatibilität	Sie können die Aktionen konfigurieren, die durchgeführt werden sollen, wenn ein Gerät gerootet wurde oder gesperrte Apps enthält. Sie können zudem Richtlinientreue für erforderliche und gesperrte Apps durchsetzen.

Funktion	Beschreibung
Proxy-Server	Sie können Android for Work-Geräte zur Verwendung eines Proxyservers für den Zugriff auf Webdienste im Netzwerk Ihres Unternehmens konfigurieren.
BlackBerry Secure Connect Plus	Sie können BlackBerry Secure Connect Plus für Android for Work-Geräte konfigurieren. BlackBerry Secure Connect Plus bietet einen sicheren IP-Tunnel zwischen geschäftlichen Apps und dem Netzwerk des Unternehmens, mit dessen Hilfe Benutzer auf Ressourcen hinter der Firewall des Unternehmens zugreifen können.
Startseitenverknüpfungen, Browserstartseite und Browserlesezeichen	Sie können eine Liste von Verknüpfungen mit Webseiten konfigurieren, die auf der Startseite von Android for Work-Geräten angezeigt werden müssen. Beispielsweise können Sie eine Verknüpfung mit einer Webseite einrichten, die Informationen zu Notfallverfahren Ihres Unternehmens enthält. Sie können außerdem die Startseite und Lesezeichen für die geschäftliche Google Chrome-App konfigurieren.

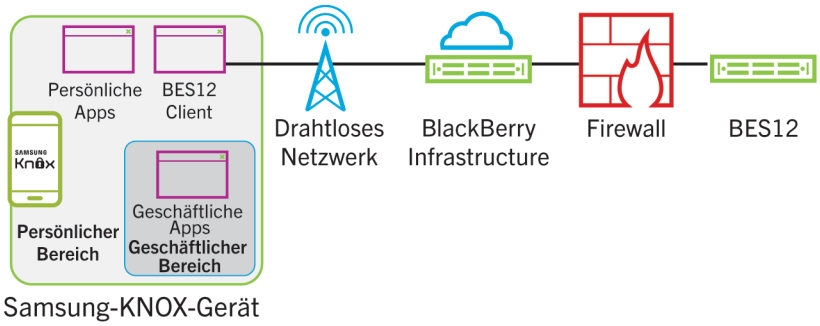
Info über KNOX Workspace

KNOX Workspace ist ein verschlüsselter kennwortgeschützter Container auf einem Samsung-Gerät für geschäftliche Apps und Daten. Er trennt die persönlichen Apps und Daten eines Benutzers von denen des Unternehmens und schützt letztere mithilfe erweiterter, von Samsung entwickelter Sicherheits- und Verwaltungsfunktionen.

Zur Verwendung von KNOX Workspace aktivieren Sie Geräte mit der Aktivierungsart „Geschäftlich und persönlich – vollständige Kontrolle (Samsung KNOX)“ oder „Nur geschäftlicher Bereich - (Samsung KNOX)“. KNOX Workspace erfordert eine Gold-Lizenz.

Weitere Informationen zu Lizenzen finden Sie in der Dokumentation zur Lizenzierung. Weitere Informationen zum KNOX Workspace finden Sie unter https://www.samsungknox.com/en/products/knox-workspace.

Architektur: KNOX Workspace



Komponente	Beschreibung
Samsung KNOX-Geräte	Ein Samsung KNOX-Gerät ist ein Samsung-Gerät, das KNOX Workspace unterstützt und mit BES12 aktiviert wird.
Persönlicher Bereich	Der persönliche Bereich auf einem Samsung KNOX-Gerät enthält die persönlichen Apps und das Android OS. Wenn Sie ein Gerät mit der Aktivierungsart „Geschäftlich und persönlich – vollständige Kontrolle (Samsung KNOX)“ aktivieren, können Sie Aspekte des persönlichen Bereichs mithilfe von IT-Richtlinienregeln verwalten.
BES12 Client	Der BES12 Client stellt eine Verbindung mit BES12 her, um Verwaltungsbefehle zu empfangen. Der BES12 Client befindet sich im persönlichen Bereich. Außerdem stellt der BES12 Client eine Verbindung mit der KLM Agent-App dem Gerät her, um die Samsung KNOX-Lizenz zu überprüfen.
Geschäftlicher Bereich	Der geschäftliche Bereich wird erstellt, wenn Sie ein Gerät in BES12 mit einer Samsung KNOX-Aktivierungsart aktivieren. Es enthält die folgenden Apps: • E-Mail-, Kontakte- und Kalender-Apps, die eine Verbindung mit dem E-Mail-Server herstellen • Google Play-App, die eine Verbindung mit dem Google Play-Store herstellt, damit Benutzer geschäftliche Apps herunterladen und installieren können • Samsung KNOX Apps-Store, der eine Verbindung mit KNOX Marketplace herstellt, damit Benutzer geschäftliche Apps herunterladen und installieren können, die nur für KNOX Workspace-Geräte verfügbar sind • Geschäftliche Apps, die eine Verbindung mit dem Unternehmensnetzwerk für den Zugriff auf Daten herstellen
BlackBerry Infrastructure	Die BlackBerry Infrastructure registriert Benutzerinformationen zur Aktivierung und Verwaltung von Geräten. Alle zwischen der BlackBerry Infrastructure und BES12 ausgetauschten Daten werden authentifiziert und mit AES-256 verschlüsselt.
BES12	BES12 ist die EMM-Lösung von BlackBerry, mit der Sie KNOX Workspace-Geräte verwalten können.

Sicherheits- und Verwaltungsfunktionen für KNOX Workspace

In der folgenden Tabelle werden einige der Sicherheits- und Verwaltungsfunktionen erläutert, die Sie bei Aktivierung von Geräten zur Verwendung von KNOX Workspace nutzen können:

Funktion	Beschreibung
Sicherheit der Hardware	Standardmäßig werden für Samsung-Geräte, die KNOX Workspace unterstützen, die folgenden Sicherheitsfunktionen für Hardware und Betriebssystem verwendet: • Secure Boot und Trusted Boot, die die Echtheit von Kernel und Betriebssystem sicherstellen • TIMA, das den Kernel überprüft und auf Änderungen überwacht
SE für Android	Standardmäßig verwenden Samsung-Geräte SE für Android. SE für Android teilt das Betriebssystem in Sicherheitsdomänen auf, damit Apps und Prozesse keinen unbefugten Zugriff auf Daten und Ressourcen erhalten. Apps außerhalb des KNOX Workspace erhalten beispielsweise keinen Zugriff auf App-Daten im geschäftlichen Bereich.
Containerverschlüsselung	Standardmäßig ist auf Samsung-Geräten der KNOX Workspace mit AES-256 verschlüsselt.
IT-Richtlinienverwaltung	BES12 unterstützt eine Reihe von IT-Richtlinienregeln zur Steuerung des KNOX Workspace. Mit IT-Richtlinienregeln können Sie Kennwortanforderungen konfigurieren, NIAP, Bluetooth-Technologie, NFC-Konnektivität, Zwei-Faktor -Authentifizierung und den Schutz für nicht gesicherte Tastaturen aktivieren usw.
Wi-Fi und VPN-Profile	BES12 unterstützt Wi-Fi- und VPN-Profile, mit deren Hilfe Sie Verbindungen mit dem Unternehmensnetzwerk konfigurieren können. BES12 unterstützt außerdem IPSec- und SSL-VPNs mit zertifikatbasierter Authentifizierung. Sie können Per App VPN-Profile konfigurieren.
E-Mail	Sie können ein E-Mail-Profil konfigurieren, durch das eine Exchange ActiveSync-Verbindung mit den geschäftlichen E-Mail- und Kalender-Apps im KNOX Workspace eingerichtet wird. Bei Bedarf können Sie die zertifikatbasierte Authentifizierung mittels SCEP konfigurieren.
BlackBerry Secure Connect Plus	Sie können BlackBerry Secure Connect Plus für KNOX Workspace-Geräte konfigurieren. BlackBerry Secure Connect Plus bietet einen sicheren IP-Tunnel zwischen geschäftlichen Apps und dem Netzwerk des Unternehmens, mit dessen Hilfe Benutzer auf Ressourcen hinter der Firewall des Unternehmens zugreifen können.
App-Verwaltung	Sie können Apps im KNOX Workspace installieren, entfernen und aktualisieren. Bei den Apps kann es sich um interne Apps oder um öffentliche, in Google Play verfügbare Apps handeln. Sie können eine Liste der zulässigen Apps im KNOX Workspace verwalten.
Kompatibilität	Sie können die Aktionen konfigurieren, die ausgeführt sollen, wenn ein Gerät gerootet wird. Sie können außerdem Richtlinientreue für erforderliche Apps durchsetzen.

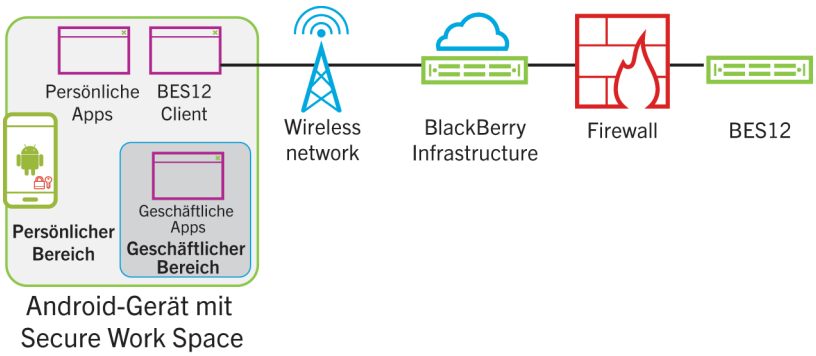
Informationen zu Secure Work Space für Android-Geräte

Secure Work Space ist ein verschlüsselter kennwortgeschützter Container für geschäftliche Apps und Daten. Er trennt die persönlichen Apps und Daten eines Benutzers von denen des Unternehmens und schützt letztere mithilfe erweiterter Sicherheits- und Verwaltungsfunktionen. Secure Work Space wurde von BlackBerry entwickelt und kann auf jedem Android-Gerät mit ARM-Prozessor und jedem iOS-Gerät ausgeführt werden.

Zur Verwendung von Secure Work Space aktivieren Sie Geräte mit der Aktivierungsart „Geschäftlich und persönlich – vollständige Kontrolle (Secure Work Space)“ oder „Geschäftlich und persönlich – Benutzer-Datenschutz (Secure Work Space)“. Secure Work Space erfordert eine Gold-Lizenz.

Weitere Informationen zu Secure Work Space finden Sie in der Dokumentation zur Sicherheit.

Architektur: Secure Work Space



Android-Gerät mit Secure Work Space

Komponente	Beschreibung
Android-Geräte	Android-Gerät, das Secure Work Space unterstützt und mit BES12 aktiviert wird
Persönlicher Bereich	Der persönliche Bereich auf einem Secure Work Space-Gerät enthält die persönlichen Apps und das Android OS. Wenn Sie ein Gerät mit der Aktivierungsart „Geschäftlich und persönlich – vollständige Kontrolle (Secure Work Space)“ aktivieren, können Sie Aspekte des persönlichen Bereichs mithilfe von IT-Richtlinienregeln verwalten. Wenn Sie ein Gerät mit der Aktivierungsart „Nur geschäftlicher Bereich (Secure Work Space)“ aktivieren, gibt es keinen persönlichen Bereich.
BES12 Client	Der BES12 Client stellt eine Verbindung mit BES12 her, um Verwaltungsbefehle zu empfangen. Der BES12 Client befindet sich im persönlichen Bereich.

Komponente	Beschreibung
Secure Work Space	Der Secure Work Space wird erstellt, wenn Sie ein Gerät in BES12 mit einer Secure Work Space-Aktivierungsart aktivieren. Er enthält die geschäftlichen Apps, die Sie zur Ausführung im geschäftlichen Bereich zulassen.
BlackBerry Infrastructure	Die BlackBerry Infrastructure registriert Benutzerinformationen zur Aktivierung und Verwaltung von Geräten. Alle zwischen der BlackBerry Infrastructure und BES12 ausgetauschten Daten werden authentifiziert und mit AES-256 verschlüsselt.
BES12	BES12 ist die EMM-Lösung von BlackBerry, mit der Sie Secure Work Space-Geräte verwalten können.

Sicherheits- und Verwaltungsfunktionen für Secure Work Space

In der folgenden Tabelle werden einige der Sicherheits- und Verwaltungsfunktionen erläutert, die Sie bei Aktivierung von Geräten zur Verwendung von Secure Work Space nutzen können:

Funktion	Beschreibung
Containerverschlüsselung	Standardmäßig ist der Secure Work Space mit AES-256 verschlüsselt.
Erkennen eines gerooteten Geräts	Wenn ein Gerät gerootet wurde, hat der Benutzer Rootzugriff auf sein Betriebssystem. BES12 erkennt, ob ein Gerät gerootet wurde. Sie können den Benutzer bitten, Rooting-Software von dem Gerät zu entfernen, oder dies erzwingen. Ein Benutzer mit einem Gerät mit Secure Work Space kann nicht auf den geschäftlichen Bereich zugreifen, wenn das Gerät gerootet wurde.
IT-Richtlinienverwaltung	BES12 unterstützt eine Reihe von IT-Richtlinienregeln zur Steuerung von Secure Work Space-Geräten. Mit IT-Richtlinienregeln können Sie Kennwortanforderungen für den geschäftlichen Bereich konfigurieren, Geräte nach Inaktivitätsperioden deaktivieren und Optionen für den geschäftlichen Browser festlegen.
Wi-Fi-Profile	BES12 unterstützt Wi-Fi-Profile, mit deren Hilfe Sie Verbindungen mit dem Unternehmensnetzwerk konfigurieren können. Secure Work Space-Geräte unterstützen VPN-Profile nicht.
E-Mail	Sie können ein E-Mail-Profil konfigurieren, durch das automatisch eine Exchange ActiveSync-, IBM Notes Traveler- oder IMAP-Verbindung mit den geschäftlichen E-Mail- und Kalender-Apps eingerichtet wird. Falls erforderlich, können Sie die zertifikatbasierte Authentifizierung über SCEP oder (nur bei Exchange ActiveSync) die Sicherheit für E-Mail mit S/MIME erhöhen.

Funktion	Beschreibung
App-Verwaltung	Sie können geschäftliche Apps auf Secure Work Space-Geräten installieren, entfernen und aktualisieren und Apps schützen. Sie können auch eine Liste zulässiger und gesperrter Apps verwalten. Gesicherte Apps sind signiert und für die Ausführung im geschäftlichen Bereich zugelassen.
Kompatibilität	Sie können die Aktionen konfigurieren, die durchgeführt werden sollen, wenn ein Gerät gerootet wurde oder gesperrte Apps enthält. Sie können zudem Richtlinientreue für erforderliche und gesperrte Apps durchsetzen.
Proxy-Server	Sie können Secure Work Space-Geräte zur Verwendung eines Proxyservers für den Zugriff auf Webdienste im Netzwerk Ihres Unternehmens konfigurieren.
Enterprise-Konnektivität	Sie können Enterprise-Konnektivität für Secure Work Space-Geräte konfigurieren. Die Enterprise-Konnektivität sendet den gesamten Datenverkehr über die BlackBerry Infrastructure an BES12. Mit Enterprise-Konnektivität vermeiden Sie eine direkte Verbindung zwischen dem Bereich hinter der Firewall Ihres Unternehmens und dem Internet.

Administratoren

Richten Sie Administratoren mit Berechtigungen ein, die ihren jeweiligen Aufgabenbereichen entsprechen.

Simple

Einrichten von Administratoren

7

Administratoren sind Benutzer, denen über ihre Benutzergruppe oder ihr Benutzerkonto eine Verwaltungsrolle zugewiesen wird. Die Aktionen, die Administratoren durchführen können, hängen von der Rolle ab, die ihnen zugewiesen ist. Sie können eine vorkonfigurierte Rolle oder eine von Ihnen erstellte benutzerdefinierte Rolle zuweisen. Jede Rolle verfügt über einen Satz Berechtigungen, mit denen die Informationen und Aufgaben festgelegt werden, die Administratoren in der BES12-Verwaltungskonsole anzeigen bzw. ausführen können.

Mit Rollen kann Ihre Organisation Folgendes erreichen:

- Geringere Sicherheitsrisiken in Zusammenhang mit der Gewährung von Zugriff auf alle Verwaltungsoptionen für alle Administratoren
- Definieren verschiedener Typen von Administratoren, um Auftragsverantwortlichkeiten besser delegieren zu können
- Höhere Effizienz für Administratoren durch die Einschränkung der verfügbaren Optionen je nach Aufgabenbereich

Schritte zum Einrichten von Administratoren

Beim Einrichten von Administratoren führen Sie die folgenden Aktionen aus:

Schritt	Aktion
1	Erstellen Sie bei Bedarf eine benutzerdefinierte Rolle.
2	Weisen Sie den Rollen bei Bedarf eine Rangordnung zu.
3	Erstellen Sie eine Benutzergruppe für Administratoren.
4	Weisen Sie einer Benutzergruppe für Administratoren eine Rolle zu.
5	Erstellen Sie ein Benutzerkonto mit einer E-Mail-Adresse, und fügen Sie es einer Administratorgruppe hinzu.

So wählt BES12 die zuzuweisende Rolle aus

Jedem Administrator wird nur eine Rolle zugewiesen. BES12 verwendet die folgenden Regeln, um zu bestimmen, welche Rolle einem Administrator zugewiesen wird:

- Die Rolle, die einem Benutzerkonto direkt zugewiesen wird, hat Vorrang vor einer indirekt von einer Benutzergruppe zugewiesenen Rolle.
- Wenn ein Administrator Mitglied mehrerer Gruppen ist, denen eine Rolle zugewiesen wurde, weist BES12 die ranghöchste Rolle zu. Sie können die Rangordnung von Rollen festlegen.

Erstellen und Verwalten von Administratorgruppen

Administratorgruppen sind Benutzergruppen, denen eine Rolle zugewiesen wird. Sie können einer per Verzeichnis verknüpften Gruppe oder einer lokalen Gruppe eine Rolle zuweisen. Ein Benutzer kann Mitglied mehrerer Administratorgruppen sein, erhält jedoch nur eine Rolle.

Nur Sicherheitsadministratoren können Mitglieder hinzufügen oder aus einer Benutzergruppe entfernen, der eine Rolle zugewiesen ist.

Erstellen einer Administratorgruppe

Wenn Sie eine Administratorgruppe erstellen, weisen Sie einer Benutzergruppe eine Rolle zu.

Bevor Sie beginnen:

- Nur Sicherheitsadministratoren können Administratorgruppen erstellen.
- Sie müssen eine Benutzergruppe für Administratoren erstellen.
- Sie müssen über eine Rolle verfügen, die zugewiesen werden kann.

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Erweitern Sie im linken Fensterbereich die Option **Administratoren**.
3. Klicken Sie auf **Gruppen**.
4. Klicken Sie auf .
5. Suchen Sie nach der Benutzergruppe, der Sie eine Rolle zuweisen möchten, und wählen Sie diese aus.
6. Klicken Sie in der Dropdown-Liste **Rolle** auf die Rolle, die Sie zuweisen möchten.
7. Klicken Sie auf **Speichern**.

BES12 sendet den Benutzern eine E-Mail-Nachricht mit deren Benutzernamen und einem Link zur Verwaltungskonsole. BES12 sendet den Benutzern zudem eine separate E-Mail-Nachricht mit deren Kennwort für die Verwaltungskonsole. Wenn ein Benutzer noch kein Konsolenkennwort hat, generiert BES12 ein temporäres Kennwort und sendet es an den Benutzer.

Wenn Sie fertig sind: Zum Hinzufügen von Benutzern zur Administratorgruppe fügen Sie diese Benutzer der Benutzergruppe hinzu, der eine Rolle zugewiesen ist. Weitere Informationen finden Sie unter „Erstellen und Verwalten von Benutzergruppen“.

Verwandte Informationen

Erstellen und Verwalten von Benutzergruppen, auf Seite 199

Zuweisen einer anderen Rolle zu einer Administratorgruppe

Bevor Sie beginnen: Nur Sicherheitsadministratoren können einer Administratorgruppe eine andere Rolle zuweisen.

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Erweitern Sie im linken Fensterbereich die Option **Administratoren**.
3. Klicken Sie auf **Gruppen**.
4. Klicken Sie auf die Administratorgruppe, die Sie ändern möchten.
5. Klicken Sie in der Dropdown-Liste **Rolle** auf die Rolle, die Sie zuweisen möchten.
6. Klicken Sie auf **Speichern**.

Entfernen einer Rolle aus einer Administratorgruppe

Wenn Sie eine Rolle aus einer Administratorgruppe entfernen, sind die Benutzer in der Gruppe keine Administratoren mehr (es sei denn, dass ihnen andere Rollen zugewiesen wurden). Die Benutzer und die Benutzergruppe verbleiben in der Verwaltungskonsole. Dies wirkt sich nicht auf die Geräte der Benutzer aus.

Bevor Sie beginnen: Nur Sicherheitsadministratoren können eine Rolle aus einer Administratorgruppe entfernen.

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Erweitern Sie im linken Fensterbereich die Option **Administratoren**.
3. Klicken Sie auf **Gruppen**.
4. Wählen Sie den Namen der Administratorgruppe aus, für die Sie eine Rolle entfernen möchten.
5. Klicken Sie auf 🗑.
6. Klicken Sie auf **Löschen**.

Erstellen und Verwalten von Administratoren

Sie können einen einzelnen Administrator erstellen, indem Sie einem Benutzerkonto eine Rolle zuweisen. Nur eine Rolle kann einem Benutzerkonto direkt zugewiesen werden.

Erstellen eines Administrators

Bevor Sie beginnen:

- Nur Sicherheitsadministratoren können Administratoren erstellen.
- Erstellen Sie ein Benutzerkonto, mit dem eine E-Mail-Adresse verknüpft ist.
- Erstellen Sie bei Bedarf eine Rolle.

1. Klicken Sie in der Menüleiste auf **Einstellungen**.

2. Erweitern Sie im linken Fensterbereich die Option **Administratoren**.
3. Klicken Sie auf **Benutzer**.
4. Klicken Sie auf .
5. Suchen Sie nach dem Benutzerkonto, dem Sie eine Rolle zuweisen möchten, und wählen Sie es aus.
6. Klicken Sie in der Dropdown-Liste **Rolle** auf die Rolle, die Sie zuweisen möchten.
7. Klicken Sie auf **Speichern**.

BES12 sendet eine E-Mail mit dem Benutzernamen und einem Link zur Verwaltungskonsole an den Benutzer. BES12 sendet dem Benutzer zudem eine separate E-Mail mit dem Kennwort für die Verwaltungskonsole. Wenn der Benutzer noch nicht über ein Konsolenkennwort verfügt, generiert BES12 ein temporäres Kennwort und sendet es an den Benutzer.

Zuweisen einer anderen Rolle zu einem Administrator

Sie können die Rolle eines anderen Administrators ändern. Sie können Ihre eigene Rolle nicht ändern.

Bevor Sie beginnen: Nur Sicherheitsadministratoren können einem Administrator eine andere Rolle zuweisen.

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Erweitern Sie im linken Fensterbereich die Option **Administratoren**.
3. Klicken Sie auf **Benutzer**.
4. Klicken Sie auf den Administrator, dessen Rolle Sie ändern möchten.
5. Klicken Sie in der Dropdown-Liste **Rolle** auf die Rolle, die Sie zuweisen möchten.
6. Klicken Sie auf **Speichern**.

Entfernen einer Rolle eines Administrators

Beim Entfernen einer Administratorrolle, entfernen Sie die Rolle, die dem Benutzerkonto direkt zugewiesen wurde. Wenn keine weiteren Rollen über die Benutzergruppe zugewiesen wurden, ist der Benutzer kein Administrator mehr. Der Benutzer ist weiterhin in der Verwaltungskonsole auffindbar, und die Geräte des Benutzers sind nicht betroffen.

Bevor Sie beginnen: Nur Sicherheitsadministratoren können eine Administratorrolle entfernen.

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Erweitern Sie im linken Fensterbereich die Option **Administratoren**.
3. Klicken Sie auf **Benutzer**.
4. Wählen Sie den Namen des Administrators aus, für den Sie eine Rolle entfernen möchten.
5. Klicken Sie auf .
6. Klicken Sie auf **Löschen**.

Anzeigen eines Anmeldungshinweises

Sie können festlegen, dass bei jedem Zugriff auf die Verwaltungskonsole durch den Administrator bzw. bei jeder Anmeldung beim BES12 Self-Service durch einen Benutzer ein Anmeldungshinweis angezeigt wird. Der Hinweis informiert den Administrator oder Benutzer über die an die Verwendung der Verwaltungskonsole oder des BES12 Self-Service geknüpften Geschäftsbedingungen. Wenn Sie festgelegt haben, dass ein Anmeldungshinweis angezeigt wird, muss der Administrator bzw. Benutzer vor der Anmeldung auf „OK“ klicken.

Anzeigen eines Anmeldungshinweises

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Erweitern Sie im linken Fensterbereich die Option **Allgemeine Einstellungen**.
3. Klicken Sie auf **Anmeldungshinweise**.
4. Klicken Sie auf .
5. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Konfigurieren des Anmeldungshinweises für die Verwaltungskonsole	Klicken Sie auf die Option **Anmeldungshinweis für die Verwaltungskonsole aktivieren**, und geben Sie im Textfeld die Informationen ein, die Administratoren beim Zugriff auf die Verwaltungskonsole angezeigt werden sollen.
Konfigurieren des Anmeldungshinweises für die BES12 Self-Service	Klicken Sie auf die Option **Anmeldungshinweis für die Selbstbedienungskonsole aktivieren**, und geben Sie im Textfeld die Informationen ein, die Benutzern beim Zugriff auf den BES12 Self-Service angezeigt werden sollen.

6. Klicken Sie auf **Speichern**.

Verwalten von Rollen

Sie können Rollen erstellen und sie Benutzerkonten oder Benutzergruppen zuweisen. Wenn Sie eine Rolle zuweisen, gewähren Sie einem Benutzer oder einer Benutzergruppe Administratorberechtigungen. Sie müssen ein Sicherheitsadministrator sein, um Rollen zu erstellen, anzuzeigen, zu ändern, ihnen einen Rang zuzuweisen oder sie zuzuweisen.

Vorkonfigurierte Rollen

In BES12 verfügt die Rolle des Sicherheitsadministrators über volle Berechtigungen für die Verwaltungskonsole – einschließlich der Erstellung und Änderung von Administratorbenutzern und -rollen. Die Rolle des Sicherheitsadministrators kann weder bearbeitet noch entfernt werden. Mindestens ein Administrator muss ein Sicherheitsadministrator sein.

BES12 enthält neben der Rolle des Sicherheitsadministrators vorkonfigurierte Rollen. Sie können alle Rollen – mit Ausnahme der Rolle des Sicherheitsadministrators – bearbeiten oder entfernen.

Wenn Sie einen Upgrade von BES5 ausgeführt haben, wurde die Rollenkonfiguration von BES5 nach BES12 kopiert.

Falls kein Upgrade von BES5 erfolgt ist, stehen die folgenden vorkonfigurierten Rollen zur Verfügung:

Rolle	Beschreibung
Sicherheitsadministrator	Volle Berechtigungen
Enterprise-Administrator	Alle Berechtigungen – mit Ausnahme der Erstellung und Änderung von Administratorbenutzern und -rollen
Senior Helpdesk	Mittlere administrative Aufgaben
Junior Helpdesk	Grundlegende administrative Aufgaben

Bewährtes Verfahren: Überprüfen der Berechtigungen jeder Rolle nach einem Upgrade von BES5

Überprüfen Sie die Berechtigungen jeder Rolle nach einem Upgrade von BES5. Bei einem Upgrade von BES5 wird die Rollenkonfiguration in BES5 nach BES12 kopiert. Da Rollen in BES12 anders funktionieren, gibt es unter Umständen Berechtigungen, die Sie hinzufügen oder entfernen möchten.

Berechtigungen für vorkonfigurierte Rollen

In den folgenden Tabellen werden die Berechtigungen aufgeführt, die für jede vorkonfigurierte Rolle in BES12 eingeschaltet werden. Die Rolle des Sicherheitsadministrators in BES12 verfügt über volle Berechtigungen für die Verwaltungskonsole – einschließlich der Verwaltung von Administratorbenutzern und -rollen.

Hinweis: Beim Upgrade von BES5 wird die Rollenkonfiguration von BES5 nach BES12 kopiert. Kopierte Rollen haben unter Umständen ähnliche Namen, aber unterschiedliche Berechtigungen.

Benutzer und Geräte

Berechtigung	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Benutzer und aktivierte Geräte anzeigen	√	√	√
Benutzer erstellen	√	√	
Benutzer bearbeiten	√	√	√
Benutzer löschen	√	√	
Benutzerliste exportieren	√		
Aktivierungskennwort generieren und E-Mail senden	√	√	√

Berechtigung	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Ein Aktivierungskennwort festlegen	√	√	√
Konsolenkennwort festlegen	√	√	√
Geräte verwalten	√	√	√
Geschäftlichen Bereich aktivieren	√	√	√
Geschäftlichen Bereich deaktivieren	√	√	√
Geschäftlichen Bereich sperren	√	√	√
Kennwort für geschäftlichen Bereich zurücksetzen	√	√	√
Gerätekennwort festlegen	√	√	√
Gerät sperren und Nachricht einrichten	√	√	√
Entsperren und Kennwort löschen	√	√	√
Nur Geschäftsdaten löschen	√	√	√
Alle Gerätedaten löschen	√	√	√
Geschäftskennwort festlegen und sperren	√	√	√
Details zum Gerätestandort anzeigen	√	√	
Verlauf des Gerätestandorts anzeigen	√		
Informationen zu Exchange Gatekeeping anzeigen	√		
Apple DEP-Geräteinformationen anzeigen	√	√	
Apple DEP-Einstellungen zuweisen	√		

Gruppen

Berechtigung	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Gruppeneinstellungen anzeigen	√	√	√
Benutzergruppen erstellen und bearbeiten	√	√	
Benutzer zu Benutzergruppen hinzufügen und daraus entfernen	√	√	
Benutzergruppen löschen	√		
Gerätegruppen erstellen und bearbeiten	√	√	
Gerätegruppen löschen	√		

Richtlinien und Profile

Berechtigung	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
IT-Richtlinien und Profile anzeigen	√	√	√
IT-Richtlinien und Profile erstellen und bearbeiten	√		
IT-Richtlinien und Profile löschen	√		
Benutzern IT-Richtlinien und Profile zuweisen	√	√	
Benutzergruppen IT-Richtlinien und Profile zuweisen	√	√	
Gerätegruppen IT-Richtlinien und Profile zuweisen	√	√	
IT-Richtlinien und Profilen einen Rang zuweisen	√		

Apps

Berechtigung	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Apps und App-Gruppen anzeigen	√	√	√
Apps und App-Gruppen erstellen und bearbeiten	√		
Apps und App-Gruppen löschen	√		
Apps und App-Gruppen zu Benutzern zuweisen	√	√	
Apps und App-Gruppen zu Benutzergruppen zuweisen	√	√	
Apps und App-Gruppen zu Gerätegruppen zuweisen	√	√	
App-Lizenzen anzeigen	√	√	√
App-Lizenzen erstellen	√		
App-Lizenzen bearbeiten	√		
App-Lizenzen löschen	√		
App-Lizenzen zu Apps oder App-Gruppen zuweisen	√	√	

Gesperrte Apps

Berechtigung	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Eingeschränkte Apps anzeigen	√	√	√
Eingeschränkte Apps erstellen	√		
Eingeschränkte Apps löschen	√		

Einstellungen

Berechtigung	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Allgemeine Einstellungen anzeigen	√	√	

Berechtigung	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Aktivierungsstandardwerte bearbeiten	√		
Aktivierungs-E-Mail bearbeiten	√		
Einstellungen für Konsolenkennwort bearbeiten	√		
Einstellungen für Selbstbedienungskonsole bearbeiten	√		
Standardvariablen bearbeiten	√		
Anmeldezustimmung bearbeiten	√		
Benutzerdefinierte Variablen bearbeiten	√		
App-Verwaltung anzeigen	√	√	√
BlackBerry World for Work bearbeiten	√		
Speicher für interne Apps bearbeiten	√		
Windows Phone-Apps bearbeiten	√		
Einstellungen für externe Integration bearbeiten	√	√	
iOS-Verwaltung bearbeiten	√		
SMTP-Servereinstellungen bearbeiten	√		
Einstellungen für das Programm zur Geräteregistrierung (DEP) von Apple bearbeiten	√		
Einstellungen für Unternehmensverzeichnis bearbeiten	√		
Einstellungen zumMicrosoft Exchange-Gatekeeping bearbeiten	√		

Berechtigung	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Android for Work-Einstellungen bearbeiten	√		
Einstellungen für Zertifizierungsstelle bearbeiten	√		
Administratorbenutzer und -rollen anzeigen	√	√	
Lizenzübersicht anzeigen	√	√	
Abonnements verwalten	√		
Lizenzeinstellungen bearbeiten	√		
Migrationseinstellungen anzeigen	√		
Migrationseinstellungen bearbeiten	√		
BlackBerry Work Connect Notification Service-Einstellungen anzeigen	√	√	
BlackBerry Work Connect Notification Service-Einstellungen bearbeiten	√		
Infrastruktureinstellungen anzeigen	√	√	
Protokollierungseinstellungen bearbeiten	√		
Serverseitige Proxyeinstellungen bearbeiten	√		
Server anzeigen	√		
Server bearbeiten	√		
Server löschen	√		
Server verwalten	√		
Überwachungseinstellungen anzeigen			

Berechtigung	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Überwachungseinstellungen und entfernte Daten bearbeiten			
BlackBerry Secure Connect Plus-Einstellungen anzeigen	√		
BlackBerry Secure Connect Plus-Einstellungen bearbeiten			
Serverzertifikate anzeigen	√		
Serverzertifikate aktualisieren	√		
SNMP-Einstellungen bearbeiten	√		
Einstellungen für Collaboration Service anzeigen	√	√	
Einstellungen für Collaboration Service bearbeiten	√		

Dashboard

Berechtigung	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Dashboard anzeigen	√	√	√

Überwachung

Berechtigung	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Überwachungsinformationen anzeigen			

BlackBerry OS-Berechtigungen

Bei einem Upgrade von BES5 stehen die folgenden zusätzlichen Berechtigungen zur Verfügung:

- BlackBerry OS-IT-Richtlinien anzeigen
- BlackBerry OS-IT-Richtlinien erstellen und bearbeiten
- BlackBerry OS-IT-Richtlinien löschen
- Aufträge anzeigen

- Aufträge bearbeiten
- Standardverteilungseinstellungen für Aufträge anzeigen
- Standardverteilungseinstellungen für Aufträge bearbeiten
- Aufgaben verwalten
- Status von Aufträgen ändern

Benutzerdefinierte Rollen

Falls die vorkonfigurierten Rollen nicht die Anforderungen Ihrer Organisation erfüllen, können Sie benutzerdefinierte Rollen für Administratoren erstellen. Außerdem können Sie benutzerdefinierte Rollen erstellen, um administrative Aufgaben auf eine definierte Liste von Benutzergruppen zu beschränken. So können Sie beispielsweise eine Rolle für neue Administratoren erstellen, die deren Berechtigungen auf eine Benutzergruppe nur zu Schulungszwecken beschränkt.

Erstellen einer benutzerdefinierten Rolle

Bevor Sie beginnen: Nur Sicherheitsadministratoren können Rollen erstellen.

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Erweitern Sie im linken Fensterbereich die Option **Administratoren**.
3. Klicken Sie auf **Rollen**.
4. Klicken Sie auf .
5. Geben Sie einen Namen und eine Beschreibung für die Rolle ein.
6. Um Berechtigungen einer anderen Rolle zu kopieren, klicken Sie auf eine Rolle in der Dropdown-Liste **Berechtigungen von Rolle übernommen**.
7. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Administratoren in dieser Rolle ermöglichen, alle Firmenverzeichnisse zu durchsuchen	1. Wählen Sie die Option **Alle Firmenverzeichnisse** aus.
Administratoren in dieser Rolle ermöglichen, ausgewählte Unternehmensverzeichnisse zu durchsuchen	1. Wählen Sie die Option **Nur ausgewählte Unternehmensverzeichnisse** aus. 2. Klicken Sie auf **Verzeichnisse auswählen**. 3. Wählen Sie ein oder mehrere Verzeichnisse aus, und klicken Sie auf . 4. Klicken Sie auf **Speichern**.

8. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Administratoren in dieser Rolle ermöglichen, alle Benutzer und Gruppen zu verwalten	1. Wählen Sie die Option **Alle Gruppen und Benutzer** aus.
Administratoren in dieser Rolle ermöglichen, ausgewählte Gruppen zu verwalten	1. Wählen Sie die Option **Nur ausgewählte Gruppen** aus. 2. Klicken Sie auf **Gruppen auswählen**. 3. Wählen Sie eine oder mehrere Gruppen aus, und klicken Sie auf →. 4. Klicken Sie auf **Speichern**.

9. Wählen Sie die Berechtigungen für Administratoren in dieser Rolle aus.
10. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Bei Bedarf passen Sie die Rangordnung der von Ihnen erstellten Rolle an.

Anzeigen der Einstellungen einer Rolle

Bevor Sie beginnen: Sie müssen ein Sicherheitsadministrator sein, um die Einstellungen einer Rolle anzuzeigen.

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Erweitern Sie im linken Fensterbereich die Option **Administratoren**.
3. Klicken Sie auf **Rollen**.
4. Klicken Sie auf die Rolle, die Sie anzeigen möchten.

Ändern der Einstellungen einer Rolle

Sie können die Einstellungen aller Rollen – mit Ausnahme der Rolle des Sicherheitsadministrators – ändern.

Bevor Sie beginnen: Sie müssen ein Sicherheitsadministrator sein, um die Einstellungen einer Rolle zu ändern.

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Erweitern Sie im linken Fensterbereich die Option **Administratoren**.
3. Klicken Sie auf **Rollen**.
4. Klicken Sie auf die Rolle, die Sie ändern möchten.
5. Klicken Sie auf ✎.
6. Geben Sie einen Namen und eine Beschreibung für die Rolle ein.
7. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Administratoren in dieser Rolle ermöglichen, alle Firmenverzeichnisse zu durchsuchen	1. Wählen Sie die Option **Alle Firmenverzeichnisse** aus.
Administratoren in dieser Rolle ermöglichen, ausgewählte Unternehmensverzeichnisse zu durchsuchen	1. Wählen Sie die Option **Nur ausgewählte Unternehmensverzeichnisse** aus. 2. Klicken Sie auf **Verzeichnisse auswählen**. 3. Wählen Sie ein oder mehrere Verzeichnisse aus, und klicken Sie auf →. 4. Klicken Sie auf **Speichern**.

8. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Administratoren in dieser Rolle ermöglichen, alle Benutzer und Gruppen zu verwalten	1. Wählen Sie die Option **Alle Gruppen und Benutzer** aus.
Administratoren in dieser Rolle ermöglichen, ausgewählte Gruppen zu verwalten	1. Wählen Sie die Option **Nur ausgewählte Gruppen** aus. 2. Klicken Sie auf **Gruppen auswählen**. 3. Wählen Sie eine oder mehrere Gruppen aus, und klicken Sie auf →. 4. Klicken Sie auf **Speichern**.

9. Ändern Sie die Berechtigungen für Administratorbenutzer in dieser Rolle.
10. Klicken Sie auf **Speichern**.

Eine Rolle löschen

Sie können alle Rollen – mit Ausnahme der Rolle des Sicherheitsadministrators – löschen.

Bevor Sie beginnen:

- Nur Sicherheitsadministratoren können Rollen löschen.
- Sie müssen alle Administratoren und Administratorgruppen aus der Rolle entfernen, die Sie löschen möchten.

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Erweitern Sie im linken Fensterbereich die Option **Administratoren**.
3. Klicken Sie auf **Rollen**.
4. Klicken Sie auf die Rolle, die Sie löschen möchten.

5. Klicken Sie auf 🗑.

Zuweisen einer Rangordnung zu Rollen

Wenn ein Administrator mehr als einer Administratorgruppe angehört, wird dem Administrator die Rolle mit dem höheren Rang zugewiesen. Wenn ein Administrator beispielsweise sowohl der Administratorgruppe „Geschäftsführer“ als auch „Abteilungsleiter“ angehört, und die Rolle „Geschäftsführer“ einen höheren Rang hat, wird dem Administrator diese Rolle zugewiesen.

Nach dem Erstellen einer benutzerdefinierten Rolle hat diese Rolle standardmäßig den niedrigsten Rang. Sie können die Rangordnung von Rollen anpassen, damit BES12 die zuzuweisende Rolle leichter auswählen kann.

Zuweisen eines Rangs zu Rollen

Bevor Sie beginnen: Nur Sicherheitsadministratoren können Rollen einen Rang zuweisen.

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Erweitern Sie im linken Fensterbereich die Option **Administratoren**.
3. Klicken Sie auf **Rollen**.
4. Verwenden Sie die Pfeile, um die Rollen in der Rangordnung nach oben oder unten zu verschieben.
5. Klicken Sie auf **Speichern**.

Secure Work Space

Trennen Sie geschäftliche und persönliche Daten auf iOS- und Android-Geräten.

Secure

Einrichten von Secure Work Space für iOS- und Android-Geräte

8

Secure Work Space ist eine Option, durch die zusätzliche Sicherheit für geschäftliche Daten auf iOS- und Android-Geräten erzielt wird. Secure Work Space ähnelt der BlackBerry Balance-Funktion auf BlackBerry 10-Geräten.

Mithilfe von Containerisierung und App-Wrapping trennt Secure Work Space durch Erstellung eines persönlichen und eines geschäftlichen Bereichs auf Geräten persönliche und geschäftliche Informationen voneinander. Sie können entscheiden, ob Sie die administrative Kontrolle über das gesamte Gerät oder nur über den geschäftlichen Bereich auf dem Gerät eines Benutzers haben möchten.

Um Secure Work Space so einzurichten, dass Benutzer Geräte mit einem geschäftlichen Bereich aktivieren können, müssen Sie die folgenden Aufgaben erfüllen:

- Erwerben von Gold-Lizenzen für Secure Work Space
- Erstellen eines Aktivierungsprofils mit der entsprechenden Aktivierungsart und Zuweisung des Profils an Benutzer oder Gruppen
- Senden von Aktivierungsinformationen an Benutzer

Wenn Benutzer ihre Geräte aktivieren, werden sie aufgefordert, einen geschäftlichen Bereich einzurichten, ein Kennwort für den geschäftlichen Bereich festzulegen und die Standard-Apps für den geschäftlichen Bereich zu installieren. Nachdem Benutzer die standardmäßigen Apps für den geschäftlichen Bereich installiert haben, können sie gesicherte Apps installieren. Gesicherte Apps werden speziell zur Ausführung im geschäftlichen Bereich von iOS- und Android-Geräten mit Secure Work Space entwickelt. Werden gesicherte Apps vor Abschluss der Einrichtung von Secure Work Space installiert, können sie nicht geöffnet werden und müssen deinstalliert werden.

Enterprise-Konnektivität und Proxy-Server

Mithilfe eines Enterprise-Konnektivitäts-Profils können Sie steuern, wie Apps auf iOS- und Android-Geräten eine Verbindung mit den Ressourcen Ihres Unternehmens herstellen. Die Enterprise-Konnektivität sendet den gesamten Datenverkehr über die BlackBerry Infrastructure an BES12. Wenn Sie für Apps im geschäftlichen Bereich einen Proxy für den Zugriff auf Webdienste im Internet oder einem Unternehmensnetzwerk verwenden, müssen Sie das Proxy-Profil dem Enterprise-Konnektivitäts-Profil zuweisen.

Enterprise-Konnektivität ist standardmäßig aktiviert. Wenn Sie Enterprise-Konnektivität deaktivieren, stellen die Apps im geschäftlichen Bereich von iOS- oder Android-Geräten die Verbindung mit den Ressourcen des Unternehmens über das interne Wi-Fi-Netzwerk oder eine auf dem Gerät konfigurierte VPN-Verbindung her.

Verwalten von Geräten mit einem geschäftlichen Bereich

Ein geschäftlicher Bereich auf Geräten hilft dabei, geschäftliche Informationen getrennt und sicher aufzubewahren, und ermöglicht die Verwaltung der geschäftlichen Daten auf Geräten. Daten im geschäftlichen Bereich werden sicher gespeichert und können nicht von außerhalb des geschäftlichen Bereichs abgerufen werden.

Weitere Informationen zum geschäftlichen Bereich finden Sie in der Dokumentation zur Sicherheit.

Wenn Benutzer ihre Geräte aktivieren, wird ein geschäftlicher Bereich auf den Geräten installiert, und die Benutzer werden aufgefordert, ein Kennwort für den geschäftlichen Bereich festzulegen. Um die Einrichtung des geschäftlichen Bereichs abzuschließen, müssen Benutzer die folgenden Apps auf ihre Geräte herunterladen:

Gerätetyp	Apps
iOS	• Work Connect: für E-Mail, Kalender, Kontakte, Notizen und Aufgaben • Work Browser: für Browsing • Documents To Go: für die sichere Anzeige und Bearbeitung von geschäftlichen Dokumenten
Android	• Work Space Manager: für das Ausführen der sonstigen Apps im geschäftlichen Bereich auf dem Gerät erforderlich • Secure Work Space: für E-Mail, Kalender, Kontakte und Browsing • Documents To Go: für die sichere Anzeige und Bearbeitung von geschäftlichen Dokumenten

Der geschäftliche Bereich gestattet Ihnen die Nutzung der folgenden Funktionen:

- Konvertieren Sie die internen Apps Ihrer Organisation in gesicherte Apps, die im geschäftlichen Bereich ausgeführt werden können, oder zum Abrufen von gesicherten Apps aus dem App Store oder von Google Play. Nutzen Sie App-Listen und App-Gruppen zur Installation von gesicherten Apps.
- Steuern Sie bestimmte Verhaltensweisen des geschäftlichen Bereichs auf Geräten, wie die Kennwortanforderungen und Verbindungvoreinstellungen, indem Sie eine IT-Richtlinie mit Benutzerkonten verknüpfen.
- Nutzen Sie IT-Administrationsbefehle zum Zurücksetzen des Kennworts für den geschäftlichen Bereich oder Löschen des geschäftlichen Bereichs auf Geräten.

Aktualisieren von Apps für den geschäftlichen Bereich

Zur Unterstützung neuer Funktionen und weiterer Betriebssysteme veröffentlicht BlackBerry neue Versionen der Apps für den geschäftlichen Bereich im App Store und in Google Play.

Benutzer sollten die Apps für den geschäftlichen Bereich aktualisieren, sobald neue Versionen verfügbar sind. Wenn Benutzer das Betriebssystem ihres Geräts aktualisieren und nicht auf die aktuelle Version der Apps für den geschäftlichen Bereich aktualisieren, funktioniert der geschäftliche Bereich möglicherweise nicht wie erwartet.

Weitere Informationen zu den unterstützten Gerätebetriebssystemen finden Sie in der Kompatibilitätsmatrix unter help.blackberry.com/detectLang/bes12/current/compatibility-matrix-pdf/.

Testen der Secure Work Space-Verbindung

Sie können die Verbindung zwischen BES12 und der Secure Work Space-Infrastruktur jederzeit testen, um sicherzustellen, dass Secure Work Space aktiviert ist.

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Klicken Sie im linken Fensterbereich unter **Externe Integration** auf **Secure Work Space**.
3. Stellen Sie sicher, dass Secure Work Space aktiviert und die Verbindung zur Secure Work Space-Infrastruktur **Erfolgreich** ist.
4. Klicken Sie optional auf **Verbindung testen**, um die Verbindung des geschäftlichen Bereichs zu testen.

Erneutes Erstellen der Secure Work Space-Verbindung

Wenn die Secure Work Space-Verbindung zur BlackBerry Infrastructure deaktiviert ist, müssen Sie die Verbindung neu erstellen.

Hierzu folgendes Beispiel: Sie erstellen mithilfe einer SRP-ID eine Testumgebung mit einem virtuellen Computer, einer BES12-Instanz, Secure Work Space und einer BES12-Datenbank. Anschließend deinstallieren Sie die Testumgebung und erstellen eine Produktionsumgebung mit derselben SRP-ID. Die Produktionsumgebung kann keine Verbindung zur BlackBerry Infrastructure herstellen, da die Secure Work Space-Verbindung, die die in der Testumgebung verwendete SRP-ID verwendet hat, in der BlackBerry Infrastructure weiterhin vorhanden ist. In diesem Fall müssen Sie die Secure Work Space-Verbindung neu erstellen.

Erneutes Erstellung der Secure Work Space-Verbindung

1. Klicken Sie in der Menüleiste auf **Einstellungen**.

2. Klicken Sie im linken Fensterbereich unter **Externe Integration** auf **Secure Work Space**.
3. Klicken Sie auf **Secure Work Space-Mandanten neu erstellen**.
   Im Fenster „Secure Work Space-Verbindung neu erstellen“ werden Sie über die Anzahl der Geräte benachrichtigt, die neu aktiviert werden müssen, wenn Sie die Secure Work Space-Verbindung neu erstellen.
4. Klicken Sie auf **Neu erstellen**.
5. Überprüfen Sie, ob Secure Work Space aktiviert ist.

Wenn Sie fertig sind: Stellen Sie sicher, dass die Benutzer ihre iOS- und Android-Geräte, die Secure Work Space verwenden, neu aktivieren.

Profile und Variablen

Erfahren Sie, wie Sie mit Profilen und Variablen Zertifikate, geschäftliche Verbindungen und Gerätestandards einrichten.

Multiplatform

Verwenden von Profilen

9

Profile enthalten Konfigurationsinformationen für Geräte; jeder Profiltyp unterstützt eine spezifische Konfiguration, z. B. Zertifikate, Einstellungen für Geschäftsverbindungen oder Einstellungen, die bestimmte Standards für Geräte durchsetzen. Sie können Einstellungen für BlackBerry 10-, iOS-, Android- und Windows Phone-Geräte in demselben Profil angeben und die Konfigurationsinformationen dann an Geräte verteilen, indem Sie Benutzerkonten, Benutzergruppen oder Gerätegruppen das Profil zuweisen.

Profile tragen dazu bei, die Geräte in Ihrer Organisation effizient zu konfigurieren. Wenn Sie viele verschiedene Einstellungen definieren oder eine große Anzahl von Geräten konfigurieren müssen, ermöglichen Ihnen Profile das Speichern aller Einstellungen für eine Konfiguration an einem Ort sowie eine schnelle Bereitstellung der Einstellungen an die entsprechenden Geräte.

Zuweisen von Profilen

Sie können Benutzerkonten, Benutzergruppen und Gerätegruppen Profile zuweisen. Einige Profiltypen verfügen möglicherweise über eine Rangfolge, um zu bestimmen, welches Profil an ein Gerät gesendet wird.

- Profiltyp mit Rangfolge: Sie können einem Benutzer ein Profil und den Gruppen, denen der Betreffende angehört, ebenfalls ein Profil zuweisen. BES12 sendet nur eines der zugewiesenen Profile an das Benutzergerät.
- Profiltyp ohne Rangfolge: Sie können einem Benutzer mehrere Profile und den Gruppen, denen der Betreffende angehört, ebenfalls mehrere Profile zuweisen. BES12 sendet alle zugewiesenen Profile an das Benutzergerät.

Hinweis: Sie können einer Gerätegruppe kein Aktivierungsprofil zuweisen.

Benutzer- oder Gruppenzuweisung	Profiltypen
Ein Profil jedes Typs kann zugewiesen werden	Die folgenden Profiltypen mit Rangfolge stehen in BES12 zur Verfügung: • Aktivierung • App-Sperrmodus • Zertifikatsabruf • Kompatibilität • CRL • Gerät • Gerätedienstanforderungen • E-Mail • Enterprise-Konnektivität • Standortbestimmung

Benutzer- oder Gruppenzuweisung	Profiltypen
	• OCSP • Proxy • Einmalige Anmeldung
Mehrere Profile jedes Typs können zugewiesen werden	Die folgenden Profiltypen ohne Rangfolge stehen in BES12 zur Verfügung: • Zertifizierungsstellenzertifikat • IMAP/POP3-E-Mail • Verwaltete Domänen • SCEP • Freigegebenes Zertifikat • Benutzeranmeldeinformationen • VPN • Webinhaltsfilter • Websymbol • Wi-Fi

Verwandte Informationen

Zuweisen eines Profils zu einer Benutzergruppe, auf Seite 204
Zuweisen eines Profils zu einem Benutzerkonto, auf Seite 219
Zuweisen eines Rangs zu Profilen, auf Seite 61

So wählt BES12 die zuzuweisenden Profile aus

Für Profiltypen mit Rangfolge sendet BES12 nur ein Profil jedes Typs an ein Gerät und verwendet vordefinierte Regeln, um zu bestimmen, welches Profil einem Benutzer und den Geräten, die der Benutzer aktiviert, zugewiesen werden soll.

Zugewiesen zu	Regeln
Benutzerkonto (Registerkarte „Benutzerzusammenfassung“ anzeigen)	1. Ein direkt einem Benutzerkonto zugewiesenes Profil hat Vorrang vor einem Profil desselben Typs, das indirekt nach Benutzergruppe zugewiesen ist. 2. Wenn ein Benutzer ein Mitglied mehrerer Benutzergruppen ist, die verschiedene Profile desselben Typs haben, weist BES12 das Profil mit der höchsten Rangordnung zu. 3. Falls zutreffend, wird das vorkonfigurierte Standardprofil zugewiesen, wenn einem Benutzerkonto kein Profil direkt oder durch Gruppenmitgliedschaft zugewiesen wird.

Zugewiesen zu	Regeln
	Hinweis: BES12 umfasst ein Standardprofil für die Enterprise-Konnektivität, ein Standard-Kompatibilitätsprofil und ein Standard-Aktivierungsprofil mit vorkonfigurierten Einstellungen für jeden Gerätetyp.
Gerät (Registerkarte „Gerät anzeigen“)	Standardmäßig erbt ein Gerät das Profil, das BES12 dem Benutzer zuweist, der das Gerät aktiviert. Wenn ein Gerät einer Gerätegruppe angehört, gelten die folgenden Regeln: 1. Ein einer Gerätegruppe zugewiesenes Profil hat Vorrang vor dem Profil desselben Typs, das BES12 einem Benutzerkonto zuweist. 2. Wenn ein Gerät ein Mitglied mehrerer Gerätegruppen ist, die verschiedene Profile desselben Typs haben, weist BES12 das Profil mit der höchsten Rangordnung zu.

BES12 muss unter Umständen in Konflikt stehende Profile auflösen, falls Sie eine der folgenden Aktionen ausführen:

- Zuweisen eines Profils zu einem Benutzerkonto, zu einer Benutzergruppe oder Gerätegruppe
- Entfernen eines Profils aus einem Benutzerkonto, aus einer Benutzergruppe oder Gerätegruppe
- Ändern der Rangordnung von Profilen
- Löschen eines Profils
- Ändern der Zugehörigkeit in einer Benutzergruppe (Benutzerkonten und verschachtelte Gruppen)
- Ändern von Geräteattributen
- Ändern der Mitgliedschaft in einer Gerätegruppe
- Löschen einer Benutzergruppe oder Gerätegruppe

Verwandte Informationen

Zuweisen eines Profils zu einer Benutzergruppe, auf Seite 204
Zuweisen eines Profils zu einem Benutzerkonto, auf Seite 219
Zuweisen eines Rangs zu Profilen, auf Seite 61

Verwalten von Profilen

10

In der Bibliothek „Richtlinien und Profile“ können Sie die Profile verwalten, die Ihre Organisation verwendet. Sie können Profile nach Rang sortieren, Informationen zu einem Profil anzeigen, die Profileinstellungen ändern, ein Profil aus Benutzerkonten oder Benutzergruppen entfernen oder ein Profil löschen.

Zuweisen eines Rangs zu Profilen

Mithilfe der Rangordnung lässt sich festlegen, welches Profil in den folgenden Szenarien BES12 an ein Gerät sendet:

- Ein Benutzer ist Mitglied in mehreren Benutzergruppen, die unterschiedliche Profile des gleichen Typs aufweisen.
- Ein Gerät ist Mitglied in mehreren Gerätegruppen, die unterschiedliche Profile des gleichen Typs aufweisen.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Erweitern Sie im linken Fensterbereich einen Profiltyp.
3. Klicken Sie auf **Rank** <***profile_type***> **Profile**.
4. Mit den Pfeiltasten können Sie die Profile in der Rangordnung nach oben oder unten verschieben.
5. Klicken Sie auf **Speichern**.

Verwandte Informationen

Zuweisen von Profilen, auf Seite 58
So wählt BES12 die zuzuweisenden Profile aus, auf Seite 59

Anzeigen eines Profils

Sie können die folgenden Informationen zu einem Profil anzeigen:

- Einstellungen, die für alle Gerätetypen gelten und die für jeden Gerätetyp individuell sind
- Liste und Anzahl der Benutzerkonten, denen das Profil zugewiesen ist (direkt und indirekt)
- Liste und Anzahl der Benutzergruppen, denen das Profil zugewiesen ist (direkt)

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Erweitern Sie im linken Fensterbereich einen Profiltyp.
3. Klicken Sie auf den Namen des Profils, das Sie anzeigen möchten.

Ändern der Profileinstellungen

Wenn Sie ein Aktivierungsprofil aktualisieren, gelten die neuen Profileinstellungen nur für zusätzliche Geräte, die ein Benutzer aktiviert. Bereits aktivierte Geräte verwenden die neuen Profileinstellungen erst, nachdem sie der Benutzer erneut aktiviert hat.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Erweitern Sie im linken Fensterbereich einen Profiltyp.
3. Klicken Sie auf den Namen des Profils, das Sie ändern möchten.
4. Klicken Sie auf .
5. Nehmen Sie Änderungen an allen allgemeinen Einstellungen vor.
6. Nehmen Sie für jeden Gerätetyp Änderungen in der jeweiligen Registerkarte vor.
7. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Ändern Sie ggf. die Rangfolge der Profile.

Entfernen eines Profils aus Benutzerkonten oder Benutzergruppen

Wenn ein Profil direkt den Benutzerkonten oder Benutzergruppen zugewiesen wurde, können Sie es aus den Benutzern oder Gruppen entfernen. Wenn ein Profil indirekt durch die Benutzergruppe zugewiesen ist, können Sie das Profil oder die Benutzerkonten aus der Gruppe entfernen. Wenn Sie ein Profil aus Benutzergruppen entfernen, wird das Profil aus jedem Benutzer entfernt, der den ausgewählten Gruppen angehört.

Hinweis: Das standardmäßige Enterprise-Konnektivitätsprofil, das Standard-Kompatibilitätsprofil und das Standard-Aktivierungsprofil können nur aus einem Benutzerkonto entfernt werden, wenn Sie es dem Benutzer direkt zugewiesen haben.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Erweitern Sie im linken Fensterbereich einen Profiltyp.
3. Klicken Sie auf den Namen des Profils, das Sie aus Benutzerkonten oder Benutzergruppen löschen möchten.
4. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Entfernen eines Profils aus Benutzerkonten	1. Klicken Sie auf die Registerkarte **Benutzern zugewiesen**. 2. Suchen Sie ggf. nach den Benutzerkonten. 3. Wählen Sie die Benutzerkonten aus, aus denen Sie das Profil entfernen möchten. 4. Klicken Sie auf .

Aufgabe	Schritte
Entfernen eines Profils aus Benutzergruppen	1. Klicken Sie auf die Registerkarte **Gruppen zugewiesen**. 2. Suchen Sie ggf. nach den Benutzergruppen. 3. Wählen Sie die Benutzergruppen aus, aus denen Sie das Profil entfernen möchten. 4. Klicken Sie auf .

Verwandte Informationen

So wählt BES12 die zuzuweisenden Profile aus, auf Seite 59

Löschen eines Profils

Wenn Sie ein Profil löschen, entfernt BES12 das Profil aus den Benutzern und Geräten, mit denen eine Verknüpfung besteht. Um ein Profil zu löschen, das anderen Profilen zugewiesen ist, müssen Sie zuvor alle vorhandenen Verknüpfungen entfernen. Bevor Sie beispielsweise ein Proxy-Profil löschen können, das mit einem VPN-Profil und einem Wi-Fi-Profil verknüpft ist, müssen Sie den Wert des verknüpften Proxy-Profils sowohl im VPN-Profil als auch im Wi-Fi-Profil ändern.

Hinweis: Sie können das standardmäßige Enterprise-Konnektivitätsprofil, das Standard-Kompatibilitätsprofil oder das Standard-Aktivierungsprofil nicht löschen.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Erweitern Sie im linken Fensterbereich einen Profiltyp.
3. Klicken Sie auf den Namen des Profils, das Sie löschen möchten.
4. Klicken Sie auf .
5. Klicken Sie auf **Löschen**.

Verwandte Informationen

So wählt BES12 die zuzuweisenden Profile aus, auf Seite 59

Verwenden von Variablen

11

BES12 unterstützt Standardvariablen und benutzerdefinierte Variablen. Standardvariablen stehen für standardmäßige Kontoattribute (z. B. Benutzername) und andere vordefinierte Attribute (z. B. die zur Geräteaktivierung verwendete Serveradresse). Sie können benutzerdefinierte Variablen verwenden, um zusätzliche Attribute zu definieren.

Sie können Variablen in Profilen verwenden sowie Benachrichtigungen zur Vorschrifteneinhaltung und Aktivierungs-E-Mail-Nachrichten individuell anpassen. Sie können Variablen verwenden, um anstatt der Angabe der tatsächlichen Werte diese zu referenzieren. Wenn das Profil, die Benachrichtigung zur Vorschrifteneinhaltung oder die Aktivierungs-E-Mail-Nachricht an die Geräte gesendet werden, werden alle Variablen durch die Werte ersetzt, die diese darstellen.

Hinweis: IT-Richtlinien unterstützen keine Variablen.

Verwenden von Variablen in Profilen

Variablen tragen in Profilen dazu bei, die Profile für die Benutzer in Ihrer Organisation effizient zu verwalten. Variablen bieten den Profilen mehr Flexibilität und können dazu beitragen, die Anzahl der Profile zu begrenzen, die Sie für jeden Profiltyp benötigen. Beispielsweise können Sie ein einzelnes VPN-Profil für mehrere Benutzer erstellen, in dem die Variable „%UserName%“ festgelegt ist, anstatt für jeden Benutzer ein separates VPN-Profil anzulegen, in dem der tatsächliche Wert des Benutzernamen angegeben wird.

Abgesehen von den Feldern „Name“ und „Beschreibung“ können Sie in jedem Textfeld eines Profils eine Variable verwenden. Beispielsweise können Sie „%UserName%@example.com“ in einem E-Mail-Profil im Feld „E-Mail-Adresse“ verwenden.

In Kompatibilitätsprofilen können Sie Variablen verwenden, um die Benachrichtigungen zur Vorschrifteneinhaltung anzupassen, die BES12 an die Benutzer versendet.

Standardvariablen

Die folgenden Standardvariablen sind in BES12 verfügbar:

Variablenname	Beschreibung	Anwendungsbereich
%ActivationPassword%	Aktivierungskennwort, das automatisch generiert oder von Ihnen für den Benutzer eingerichtet wird	Meldungen der Aktivierungs-E-Mail
%ActivationPasswordExpiry%	Datum und Uhrzeit des Ablaufs des Aktivierungskennworts	Meldungen der Aktivierungs-E-Mail
%ActivationURL%	Webadresse des Servers, der die Aktivierungsanforderung empfängt	Meldungen der Aktivierungs-E-Mail

Variablenname	Beschreibung	Anwendungsbereich
%ActivationUserName%	Benutzername für Aktivierungsanforderungen Entspricht %UserEmailAddress% (falls verfügbar für einen Benutzer) oder SRP ID\%UserName%	Meldungen der Aktivierungs-E-Mail
%AdminPortalURL%	Webadresse der BES12-Verwaltungskonsole	E-Mail-Nachrichten Administratorzugriff (kann nicht vom Benutzer definiert werden)
%ComplianceApplicationList%	Liste der Apps, die gegen Kompatibilitätsregeln verstoßen (nicht zugewiesene Apps sind installiert, erforderliche Apps sind nicht installiert oder gesperrte Apps sind installiert)	Benachrichtigungen zur Vorschrifteneinhaltung
%ComplianceEnforcementAction%	Erzwingungsaktion, die BES12 durchführt, wenn ein Gerät nicht konform ist	Benachrichtigungen zur Vorschrifteneinhaltung
%ComplianceEnforcementActionWithDescription%	Erzwingungsaktion, die BES12 durchführt, wenn ein Gerät nicht konform ist, ergänzt durch eine Beschreibung der Erzwingungsaktion	Benachrichtigungen zur Vorschrifteneinhaltung
%ComplianceRuleViolated%	Kompatibilitätsregel, gegen die ein Gerät verstoßen hat	Benachrichtigungen zur Vorschrifteneinhaltung
%DeviceIMEI%	International Mobile Equipment Identity-Nummer (IMEI) eines Geräts	Profile
%DeviceModel%	Modellnummer eines Geräts	Benachrichtigungen zur Vorschrifteneinhaltung
%SSLCertName%	Common Name des sicheren Kommunikationszertifikats	Meldungen der Aktivierungs-E-Mail
%SSLCertSHA%	Fingerabdruck des sicheren Kommunikationszertifikats	Meldungen der Aktivierungs-E-Mail
%UserDisplayName%	Anzeigename eines Benutzers	Meldungen der Aktivierungs-E-Mail
%UserDistinguishedName%	Distinguished Name des Verzeichnisbenutzers Bei einem lokalen Benutzer identisch mit %UserName%	Profile
%UserDomain%	Microsoft Active Directory-Domäne, der ein Verzeichnisbenutzer angehört	Profile

Variablenname	Beschreibung	Anwendungsbereich
%UserEmailAddress%	E-Mail-Adresse eines Benutzers	Aktivierungs-E-Mail-Nachrichten, Profile
%UserName%	Benutzername eines Benutzers	Aktivierungs-E-Mail-Nachrichten, Profile
%UserPrincipalName%	Prinzipalname des Verzeichnisbenutzers Bei einem lokalen Benutzer identisch mit %UserEmailAddress%	Profile
%UserSelfServicePortalURL%	Webadresse von BES12 Self-Service	Meldungen der Aktivierungs-E-Mail

Wenn Sie eine hohe Verfügbarkeit für die Verwaltungskonsole in der BES12-Domäne konfigurieren, empfiehlt es sich, die Variablen %AdminPortalURL% und %UserSelfServicePortal% zu aktualisieren. Weitere Informationen finden Sie in der Dokumentation zur Konfiguration.

Benutzerdefinierte Variablen

Sie verwenden Kennzeichen, um die Attribute und Kennwörter zu definieren, die von den benutzerdefinierten Variablen dargestellt werden. Beispielsweise können Sie „VPN-Kennwort“ als Kennzeichen für die Variable „%custom_pswd1%“ verwenden. Wenn Sie ein Benutzerkonto erstellen oder aktualisieren, werden die Kennzeichen als Feldnamen verwendet, und Sie legen die entsprechenden Werte für die benutzerdefinierten Variablen fest, die Ihre Organisation verwendet. Alle Benutzerkonten, einschließlich der Administrator-Benutzerkonten, unterstützen benutzerdefinierte Variablen.

Benutzerdefinierte Variablen unterstützen Textwerte oder maskierte Textwerte. Aus Sicherheitsgründen sollten Sie benutzerdefinierte Variablen verwenden, die maskierte Textwerte zur Darstellung von Kennwörtern unterstützen.

Die folgenden benutzerdefinierten Variablen sind in BES12 verfügbar:

Variablenname	Beschreibung
%custom1%, %custom2%, %custom3%, %custom4%, %custom5%	Sie können bis zu fünf verschiedene Variablen für die von Ihnen definierten Attribute nutzen (Textwerte).
%custom_pswd1%, %custom_pswd2%, %custom_pswd3%, %custom_pswd4%, %custom_pswd5%	Sie können bis zu fünf verschiedene Variablen für die von Ihnen definierten Kennwörter nutzen (maskierte Textwerte).

Definieren von benutzerdefinierten Variablen

Bevor Sie benutzerdefinierte Variablen verwenden können, müssen Sie diese definieren. Wenn Sie ein Benutzerkonto erstellen oder aktualisieren werden nur die benutzerdefinierten Variablen angezeigt, die über ein Kennzeichen verfügen.

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Erweitern Sie im linken Fensterbereich die Option **Allgemeine Einstellungen**.
3. Klicken Sie auf **Benutzerdefinierte Variablen**.
4. Aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Variablen beim Hinzufügen oder Bearbeiten eines Benutzers anzeigen**.
5. Legen Sie ein Kennzeichen für jede benutzerdefinierte Variable fest, die Sie verwenden möchten. Die Kennzeichen werden als Feldnamen im Abschnitt **Benutzerdefinierte Variablen** verwendet, wenn Sie ein Benutzerkonto erstellen oder aktualisieren.
6. Klicken Sie auf **Speichern**.

Verwenden von benutzerdefinierten Variablen

Nachdem Sie die benutzerdefinierten Variablen definiert haben, müssen Sie die entsprechenden Werte festlegen, wenn Sie ein Benutzerkonto erstellen oder aktualisieren. Sie können die benutzerdefinierten Variablen dann auf die gleiche Weise wie Standardvariablen verwenden. Sie legen den Namen der Variablen fest, wenn Sie Profile oder Benachrichtigungen zur Vorschrifteneinhaltung sowie Aktivierungs-E-Mail-Nachrichten anpassen oder erstellen.

Beispiel: Verwendung des gleichen VPN-Profils für mehrere Benutzer, die jeweils eigene VPN-Kennwörter haben

In dem folgenden Beispiel ist „VPN-Kennwort“ das Kennzeichen, das Sie für die Variable „%custom_pswd1%“ festgelegt haben. Wenn Sie ein Benutzerkonto aktualisieren, wird dieses Kennzeichen als Feldname im Abschnitt „Benutzerdefinierte Variablen“ verwendet.

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte**.
2. Suchen Sie nach einem Benutzerkonto.
3. Klicken Sie in den Suchergebnissen auf den Namen eines Benutzerkontos.
4. Klicken Sie auf der Registerkarte **Benutzerzusammenfassung** im Abschnitt **Benutzerdaten** auf .
5. Erweitern Sie **Benutzerdefinierte Variablen**.
6. Geben Sie im Feld **VPN-Kennwort** ein VPN-Kennwort für einen Benutzer ein.
7. Klicken Sie auf **Speichern**.
8. Wiederholen Sie die Schritte 2 bis 7 für alle Benutzer, die das VPN-Profil verwenden werden.
9. Wenn Sie das VPN-Profil erstellen, geben Sie im Feld **Kennwort %custom_pswd1%** ein.

Zertifikate

Senden Sie alle erforderlichen Zertifikate an Geräte.

Simple

Verwalten von Zertifikaten mithilfe von Profilen

12

Sie können Zertifikate mithilfe von Profilen verwalten, die in der Bibliothek der Richtlinien und Profile verfügbar sind.

Je nach Gerätefunktionen und Aktivierungsart können Sie folgende Profile zum Senden von Zertifikaten an Geräte verwenden:

Profil	Beschreibung
Zertifizierungsstellenzertifikat	Ein Profil mit Zertifizierungsstellenzertifikat legt ein Zertifizierungsstellenzertifikat fest, das die Geräte verwenden können, damit das geschäftliche Netzwerk oder der Server als vertrauenswürdig gilt.
SCEP	Ein SCEP-Profil legt fest, wie die Geräte Zertifikate beziehen, die bei einem geschäftlichen Netzwerk oder Mailserver unter Verwendung von SCEP-Diensten zur Authentifizierung verwendet werden.
Profile für Benutzeranmeldeinformationen	Mit einem Profil für Benutzeranmeldeinformationen können Sie festlegen, wie Zertifikate auf Geräten bereitgestellt werden, wenn im Unternehmen Entrust-Software für PKI-Dienste verwendet wird.
Freigegebenes Zertifikat	Ein Profil für ein freigegebenes Zertifikat legt ein Client-Zertifikat fest, das iOS und Android-Geräte verwenden können, um Benutzer bei einem geschäftlichen Netzwerk oder einem Server zu authentifizieren. BES12 sendet das gleiche Client-Zertifikat an jeden Benutzer, dem das Profil zugewiesen ist.

Senden von Zertifikaten an Geräte

13

Ein Zertifikat ist ein digitales Dokument, das von einer Zertifizierungsstelle erstellt wurde, die Identität eines Zertifikatempfängers überprüft und diese mit einem öffentlichen Schlüssel verknüpft. Für jedes Zertifikat ist ein entsprechender privater Schlüssel vorhanden, der getrennt gespeichert wird. Der öffentliche Schlüssel und der private Schlüssel bilden ein asymmetrisches Schlüsselpaar, das zur Datenverschlüsselung und zur Identitätsauthentifizierung verwendet werden kann. Eine Zertifizierungsstelle signiert das Zertifikat und bescheinigt, dass Institutionen, die der Zertifizierungsstelle vertrauen, auch dem Zertifikat vertrauen können.

Je nach Gerätefunktionen und Aktivierungsart können Zertifikate auf Geräten für Folgendes verwendet werden:

- Authentifizieren mittels SSL/TLS, wenn eine Verbindung zu Webseiten hergestellt wird, die HTTPS verwenden
- Authentifizieren mit einem geschäftlichen Mailserver
- Authentifizieren mit einem geschäftlichen Wi-Fi-Netzwerk oder einem VPN
- Verschlüsseln und Signieren von E-Mail-Nachrichten mittels S/MIME-Schutz

Viele Zertifikate, die für verschiedene Zwecke verwendet werden, können auf einem Gerät gespeichert werden. Sie können auch Zertifikatsprofile verwenden, um Zertifizierungsstellenzertifikate und Client-Zertifikate an Geräte zu senden.

Verwandte Informationen
Hinzufügen eines Client-Zertifikats zu einem Benutzerkonto, auf Seite 220

Erstellen von Profilen mit Zertifizierungsstellenzertifikat

Sie müssen möglicherweise Zertifizierungsstellenzertifikate an Geräte verteilen, wenn Ihre Organisation S/MIME verwendet oder wenn die Geräte eine zertifikatsbasierte Authentifizierung für die Verbindung mit einem Netzwerk oder einem Server in Ihrer Organisationsumgebung verwenden.

Wenn Sie ein Zertifizierungsstellenzertifikat an ein Gerät senden, vertraut das Gerät dem mit einem von der Zertifizierungsstelle erstellten Cyber- oder Serverzertifikat. Wenn die von der Zertifizierungsstelle ausgegebenen Netzwerk- und Serverzertifikate Ihrer Organisation auf Geräten gespeichert werden, ist die Vertrauenswürdigkeit beim Aufbau sicherer Verbindungen zu Ihren Netzwerken und Servern gewährleistet. Wenn das Zertifizierungsstellenzertifikat, das die S/MIME-Zertifikate Ihrer Organisation unterzeichnet hat, auf Geräten gespeichert wird, können die Geräte dem Zertifikat des Senders vertrauen, wenn eine E-Mail eingeht.

Viele Zertifizierungsstellenzertifikate, die für verschiedene Zwecke verwendet werden, können auf einem Gerät gespeichert werden. Mithilfe von Profilen mit Zertifizierungsstellenzertifikat können Sie Zertifizierungsstellenzertifikate an Geräte senden.

Erstellen eines Profils mit Zertifizierungsstellenzertifikat

Bevor Sie beginnen: Sie müssen eine Zertifizierungsstellen-Zertifikatdatei abrufen, die Sie an die Geräte senden möchten. Diese muss über die Dateierweiterung .DER verfügen.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf + neben **Zertifizierungsstellenzertifikat**.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein. Jedes Profil mit Zertifizierungsstellenzertifikat muss über einen eindeutigen Namen verfügen. Einige Namen (z. B. ca_1) sind reserviert.
4. Klicken Sie im Feld **Zertifikatsdatei** auf **Durchsuchen**, um die Zertifikatsdatei zu finden.
5. Wenn das Zertifizierungsstellenzertifikat an BlackBerry-Geräte gesendet wird, geben Sie einen oder mehrere der folgenden Zertifikatspeicher an, um das Zertifikat an das Gerät zu senden:
    - Browser-Zertifikatspeicher
    - VPN-Zertifikatspeicher
    - Wi-Fi-Zertifikatspeicher
    - Unternehmens-Zertifikatspeicher
6. Klicken Sie auf **Hinzufügen**.

Speicher für Zertifizierungsstellenzertifikate auf BlackBerry 10-Geräten

Zertifizierungsstellenzertifikate, die an BlackBerry 10-Geräte gesendet werden, können je nach dem Zweck in unterschiedlichen Zertifikatspeichern gespeichert werden.

Speicher	Beschreibung
Browser-Zertifikatspeicher	Der geschäftliche Browser auf BlackBerry 10-Geräten nutzt die Zertifikate in diesem Speicher, um SSL-Verbindungen zu Servern in Ihrer Organisationsumgebung herzustellen.
VPN-Zertifikatspeicher	BlackBerry 10-Geräte nutzen Zertifikate in diesem Speicher für VPN-Verbindungen. Sie müssen die Einstellung „Quelle des vertrauenswürdigen Zertifikats“ im VPN-Profil auf „Speicher vertrauenswürdiger Zertifikate“ festlegen, um die Zertifikate in diesem Speicher für geschäftliche VPN-Verbindungen nutzen zu können.
Wi-Fi-Zertifikatspeicher	BlackBerry 10-Geräte nutzen Zertifikate in diesem Speicher für Wi-Fi-Verbindungen. Sie müssen die Einstellung „Quelle des vertrauenswürdigen Zertifikats“ im Wi-Fi-Profil auf „Speicher vertrauenswürdiger Zertifikate“ festlegen, um die Zertifikate in diesem Speicher für Wi-Fi-Geschäftsverbindungen nutzen zu können.

Speicher	Beschreibung
Unternehmens-Zertifikatspeicher	BlackBerry 10-Geräte nutzen die Zertifikate in diesem Speicher, um eingehende S/MIME-geschützte E-Mail-Nachrichten zu authentifizieren.

Erstellen von SCEP-Profilen

Sie können ein SCEP-Profil verwenden, um anzugeben, wie BlackBerry 10-, iOS- und Android-Geräte mit Secure Work Space, Android for Work, KNOX Workspace oder KNOX MDM-Aktivierung Zertifikate über einen SCEP-Dienst aus der Zertifizierungsstelle Ihrer Organisation abrufen. SCEP ist ein IETF-Protokoll, das das Anmelden von Zertifikaten auf vielen Geräten vereinfacht, indem zur Ausstellung der einzelnen Zertifikate weder ein Eingriff vonseiten des Administrators noch eine Genehmigung erforderlich sind. Geräte können SCEP verwenden, um Client-Zertifikate von einer SCEP-kompatiblen Zertifizierungsstelle, die Ihre Organisation verwendet, anzufordern und abzurufen. Die von Ihnen verwendete Zertifizierungsstelle muss Challenge-Kennwörter unterstützen. Die Zertifizierungsstelle verifiziert mithilfe von Challenge-Kennwörtern, dass das Gerät zum Senden einer Zertifikatanforderung autorisiert ist.

Je nach Gerätefunktionen und Aktivierungsart können Geräte die über SCEP abgerufenen Zertifikate für die zertifikatbasierte Authentifizierung in einem Browser oder zum Herstellen einer Verbindung mit einem geschäftlichen Wi-Fi-Netzwerk, einem geschäftlichen VPN oder einem E-Mail-Server verwenden.

Auf iOS- und Android-Geräten mit Secure Work Space muss das SCEP-Profil einem E-Mail Profil oder einem Wi-Fi-Profil zugewiesen sein, damit es per Push auf das Gerät übertragen wird. Auf Android for Work-Geräten können mit einem SCEP-Profil erstellte Zertifikate nicht für die zertifikatbasierte Authentifizierung beim geschäftlichen Wi-Fi-Netzwerk oder dem E-Mail-Server verwendet werden.

Windows Phone-Geräte unterstützen SCEP nicht.

Erstellen eines SCEP-Profils

Die erforderlichen Profileinstellungen sind je nach Gerätetyp unterschiedlich und hängen von der SCEP-Dienstkonfiguration in der Umgebung Ihrer Organisation ab.

Bevor Sie beginnen: Wenn Sie Geräten Entrust-Client-Zertifikate mithilfe eines SCEP-Profils bereitstellen möchten, führen Sie die Anweisungen in „Integration von BES12 mit der Entrust-Software Ihres Unternehmens“ aus.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf + neben **SCEP**.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
4. Geben Sie im Feld **URL** die URL für den SCEP-Dienst ein. Die URL sollte das Protokoll, den FQDN, die Portnummer und den SCEP-Pfad enthalten.
5. Geben Sie im Feld **Instanzname** den Instanznamen der Zertifizierungsstelle ein.
6. Führen Sie in der Dropdown-Liste **Zertifizierungsstellenverbindung** eine der folgenden Aktionen aus:

- Um eine von Ihnen konfigurierte Entrust-Verbindung zu verwenden, klicken Sie auf die entsprechende Verbindung. Klicken Sie in der Dropdown-Liste **Profil** auf ein digitales ID-Profil. Geben Sie die Werte für das digitale ID-Profil an.
- Um eine andere Zertifizierungsstelle zu verwenden, klicken Sie auf **Generisch**. Wählen Sie in der Liste **SCEP-Abfragetyp** entweder **Statisch** oder **Dynamisch** aus, und geben Sie dann die erforderlichen Einstellungen für den Abfragetyp an.

7. Deaktivieren Sie optional das Kontrollkästchen für alle Gerätetypen, für die Sie das Profil nicht konfigurieren möchten.
8. Führen Sie folgende Aktionen aus:
   a. Klicken Sie auf die Registerkarte eines Gerätetyps.
   b. Konfigurieren Sie die entsprechenden Werte für jede Profileinstellung so, dass sie der SCEP-Dienstkonfiguration in der Umgebung Ihres Unternehmens entsprechen.
9. Wiederholen Sie Schritt 8 für jeden Gerätetyp in Ihrer Organisation.
10. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Wenn Geräte das Zertifikat zur Authentifizierung bei einem geschäftlichen Wi-Fi-Netzwerk, geschäftlichen VPN oder einem geschäftlichen Mailserver verwenden, verknüpfen Sie das SCEP-Profil mit einem Wi-Fi-, VPN- oder E-Mail-Profil.

Verwandte Informationen
SCEP-Profileinstellungen, auf Seite 355
Integration von BES12 mit der Entrust-Software Ihrer Organisation, auf Seite 76

Erstellen von Profilen für freigegebene Zertifikate

Wenn Sie Verbindungen zu Netzwerken oder Servern in der Umgebung Ihrer Organisation mithilfe einer zertifikatbasierten Authentifizierung herstellen, müssen Sie möglicherweise BES12 verwenden, um Client-Zertifikate an Geräte zu senden.

Durch Profile für freigegebene Zertifikate werden Clientzertifikate an iOS- und Android-Geräte mit MDM-Steuerelemente-Aktivierung und an Android-Geräte mit KNOX Workspace oder Android for Work gesendet. Die Geräte können das Client-Zertifikat zur Authentifizierung gegenüber einem Netzwerk oder Server in Ihrer Organisationsumgebung vorlegen. Sie sollten Profile für freigegebene Zertifikate nur dann nutzen, wenn Sie mehr als einem Benutzer die gemeinsame Nutzung eines Client-Zertifikats ermöglichen möchten.

Wenn Ihr Unternehmen einen SCEP-Dienst nutzt, können Sie auch SCEP-Profile verwenden, um Client-Zertifikate auf BlackBerry 10-Geräten, iOS-Geräten und Android-Geräten mit Secure Work Space-, KNOX Workspace- oder KNOX MDM-Aktivierung zu registrieren.

Um für jeden Benutzer ein separates Client-Zertifikat zu erstellen, können Sie auf der Registerkarte „Benutzerzusammenfassung“ einem Benutzerkonto ein Client-Zertifikat hinzufügen, und BES12 sendet das Zertifikat an das iOS des Benutzers sowie an die Android-Geräte. Weitere Informationen finden Sie unter „Hinzufügen eines Client-Zertifikats zu einem Benutzerkonto“.

Verwandte Informationen

Hinzufügen eines Client-Zertifikats zu einem Benutzerkonto, auf Seite 220

Erstellen eines Profils für ein freigegebenes Zertifikat

Bevor Sie beginnen: Sie müssen die Client-Zertifikatdatei abrufen, die Sie an die Geräte senden möchten. Diese muss über die Dateierweiterung .pfx oder .p12 verfügen.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf + neben **Freigegebenes Zertifikat**.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein. Jedes Profil eines freigegebenen Zertifikats muss über einen eindeutigen Namen verfügen. Einige Namen (z. B. ca_1) sind reserviert.
4. Geben Sie im Feld **Kennwort** ein Kennwort für das Profil des freigegebenen Zertifikats ein.
5. Klicken Sie im Feld **Zertifikatsdatei** auf **Durchsuchen**, um die Zertifikatsdatei zu finden.
6. Klicken Sie auf **Hinzufügen**.

Integration von BES12 mit der Entrust-Software Ihrer Organisation

14

Wenn Ihre Organisation zur Bereitstellung von PKI-Diensten die Entrust-Software verwendet, können Sie die zertifikatsbasierte Entrust-Authentifizierung auf die Geräte ausweiten, die mithilfe von BES12 verwaltet werden.

Entrust-Produkte wie Entrust IdentityGuard und Entrust Authority Administration Services stellen Client-Zertifikate zur Verfügung. Sie können mithilfe von BES12 eine Verbindung zum Entrust-Produkt Ihrer Organisation konfigurieren und das Entrust-Zertifizierungsstellenzertifikat sowie Client-Zertifikate für Geräte bereitstellen. Geräte können Client-Zertifikate für SSL-Verbindungen mit Webseiten, zur Authentifizierung bei einem geschäftlichen Mailserver, Wi-Fi-Netzwerk oder VPN und für die Verschlüsselung und Signatur von E-Mail-Nachrichten mittels S/MIME verwenden.

Schritte zur Integration von BES12 mit der Entrust-Software Ihrer Organisation

Führen Sie folgende Aktionen aus, um BES12 mit der Entrust-Software Ihrer Organisation zu integrieren:

Schritt	Aktion
1	Stellen Sie eine Verbindung zwischen BES12 und der Entrust-Software Ihrer Organisation her.
2	Verwenden Sie ggf. ein Profil mit Zertifizierungsstellenzertifikat, um das Entrust-Zertifizierungsstellenzertifikat an die Geräte zu senden.
3	Richten Sie ein Profil für die Bereitstellung von Entrust-Client-Zertifikaten an Geräte ein. Der Profiltyp (SCEP oder Benutzeranmeldeinformationen) wird durch die Verwendungsart der Entrust-Software und die von Ihrer Organisation unterstützten Gerätetypen bestimmt.
4	Fügen Sie ggf. das SCEP- bzw. Benutzeranmeldeinformations-Profil zu den Wi-Fi-, VPN- oder E-Mail-Profilen hinzu.
5	Weisen Sie die Profile Benutzergruppen und Benutzerkonten zu.

Hinzufügen einer Verbindung zur Entrust-Software Ihrer Organisation

Um BES12 mit der Entrust-Software Ihrer Organisation zu integrieren, müssen Sie eine Verbindung zu Entrust IdentityGuard bzw. Entrust Authority Administration Services hinzufügen.

Bevor Sie beginnen: Kontaktieren Sie den Entrust-Administrator Ihrer Organisation, um die URL des Entrust MDM Web Service und die Anmeldeinformationen für ein Entrust-Administratorkonto zu erhalten, das Sie zum Herstellen einer Verbindung zwischen BES12 und der Entrust-Software verwenden können.

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Klicken Sie im linken Fensterbereich auf **Externe Integration** > **Zertifizierungsstelle**.
3. Klicken Sie auf **Hinzufügen einer Entrust-Verbindung**.
4. Geben Sie im Feld **Verbindungsname** einen Namen für die Verbindung ein.
5. Geben Sie im Feld **URL** die URL für den Entrust MDM Web Service ein.
6. Geben Sie im Feld **Benutzername** den Benutzernamen des Entrust-Administratorkontos ein.
7. Geben Sie im Feld **Kennwort** das Kennwort für das Entrust-Administratorkonto ein.
8. Klicken Sie auf **Verbindung testen**.
9. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind:

- Um eine Verbindung zu bearbeiten, klicken Sie auf den Verbindungsnamen.
- Um eine Verbindung zu entfernen, klicken Sie auf ✕.

Senden der Entrust-Zertifizierungsstellenzertifikate an Geräte

Wenn Ihre Organisation erfordert, dass Benutzergeräte das Entrust-Zertifizierungsstellenzertifikat zur Authentifizierung beim geschäftlichen Netzwerk, zur Herstellung von SSL-Verbindungen zu Webseiten oder für andere Zwecke verwenden, können Sie das Entrust-Zertifizierungsstellenzertifikat mithilfe eines Zertifizierungsstellenzertifikat-Profils an die Geräte senden.

Kontaktieren Sie den Entrust-Administrator Ihrer Organisation, um das Entrust-Zertifizierungsstellenzertifikat zu erhalten. Weitere Informationen zum Erstellen eines Profils mit Zertifizierungsstellenzertifikat finden Sie unter „Erstellen von Profilen mit Zertifizierungsstellenzertifikat“.

Bereitstellung von Entrust-Client-Zertifikaten an Geräte

Sie können für die Bereitstellung von Entrust-Client-Zertifikaten verschiedene Profiltypen verwenden. Der ausgewählte Profiltyp hängt von der Verwendungsart der Entrust-Software, den von Ihrer Organisation unterstützten Geräten und den zu verwaltenden Zertifikaten ab.

Wenn mehrere Profile verfügbar sind, wählen Sie jeweils nur einen Profiltyp aus.

Gerät	Mailserver-Authentifizierung (Exchange ActiveSync)	Signatur und Verschlüsselung von Nachrichten (S/MIME)	Wi-Fi-Authentifizierung	VPN-Authentifizierung
BlackBerry 10*	• SCEP-Profil • Profil für Benutzeranmeldeinformationen	Konfiguration durch Benutzer	• SCEP-Profil • Profil für Benutzeranmeldeinformationen	• SCEP-Profil • Profil für Benutzeranmeldeinformationen
iOS	• SCEP-Profil • Profil für Benutzeranmeldeinformationen	• SCEP-Profil • Profil für Benutzeranmeldeinformationen	• SCEP-Profil • Profil für Benutzeranmeldeinformationen	• SCEP-Profil • Profil für Benutzeranmeldeinformationen
Android	• SCEP-Profil** • Profil für Benutzeranmeldeinformationen	Nicht unterstützt	• SCEP • Profil für Benutzeranmeldeinformationen	Nicht unterstützt
Geräte mit KNOX Workspace	• SCEP-Profil • Profil für Benutzeranmeldeinformationen	Nicht unterstützt	• SCEP-Profil • Profil für Benutzeranmeldeinformationen	• SCEP-Profil • Profil für Benutzeranmeldeinformationen
Geräte mit KNOX MDM	• SCEP-Profil • Profil für Benutzeranmeldeinformationen	Nicht unterstützt	• SCEP-Profil • Profil für Benutzeranmeldeinformationen	Nicht unterstützt
Windows Phone	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt

Gerät	Mailserver-Authentifizierung (Exchange ActiveSync)	Signatur und Verschlüsselung von Nachrichten (S/MIME)	Wi-Fi-Authentifizierung	VPN-Authentifizierung
Android for Work	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt

* Profile für Benutzeranmeldeinformationen erfordern BlackBerry 10 OS Version 10.3.1 oder höher. BlackBerry 10-Geräte können Nachrichten mittels S/MIME signieren und verschlüsseln; diese Funktion muss vom Gerätebenutzer jedoch aktiviert und konfiguriert werden (Sie können die erforderlichen Zertifikate an die Geräte senden).

** SCEP-Profile werden auf Android-Geräten mit Secure Work Space und Geräten, für die KNOX Workspace oder KNOX MDM verwendet wird, unterstützt. Android mit Secure Work Space unterstützt SCEP-Profile nur dann, wenn das Profil einem E-Mail Profil zugewiesen ist.

Profile mit Benutzeranmeldeinformationen ermöglichen das Abrufen von Client-Zertifikaten über Geräte von der Entrust-Zertifikatstelle. SCEP-Profile bieten dieselbe Funktion mit erweiterten Optionen für die Kommunikation zwischen Geräten und der Entrust-Zertifikatsstelle. Profile mit Benutzeranmeldeinformationen und SCEP-Profile ermöglichen eine automatische Erneuerung der Client-Zertifikate über Geräte, bevor sie ablaufen.

Verwandte Informationen

Erstellen eines Profils mit Benutzeranmeldeinformationen, auf Seite 79

Erstellen eines Profils mit Benutzeranmeldeinformationen

Bevor Sie beginnen:

- Kontaktieren Sie den Entrust-Administrator Ihrer Organisation, um zu bestimmen, welche digitalen ID-Profile Sie an Geräte senden sollten. BES12 stellt eine Liste mit digitalen ID-Profilen, basierend auf den durch den Entrust-Administrator vorgenommenen Konfigurationen, zur Verfügung.
- Digitale ID-Profile, die Signatur- und Verschlüsselungsschlüssel für S/MIME enthalten, werden von Profilen mit Benutzeranmeldeinformationen nicht unterstützt. Der Entrust-Administrator muss zwei separate digitale ID-Profile konfigurieren; ein Profil für die Signatur und ein Profil für die Verschlüsselung.
- Fragen Sie den Entrust-Administrator, welche digitalen ID-Werte bereitgestellt werden müssen, beispielsweise die Werte für Gerätetypen (devicetype), Entrust IdentityGuard-Gruppen (iggroup) und Entrust IdentityGuard-Benutzernamen (igusername).

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie im linken Fensterbereich auf + neben **Benutzeranmeldeinformationen**.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
4. Klicken Sie in der Dropdown-Liste **Zertifizierungsstellenverbindung** auf die konfigurierte Entrust-Verbindung.
5. Klicken Sie in der Dropdown-Liste **Profil** auf das entsprechende digitale ID-Profil.
6. Geben Sie die Werte für das digitale ID-Profil an.

7. Wenn Geräte für die Verschlüsselung von E-Mail-Nachrichten mittels S/MIME Client-Zertifikate verwenden und der Zugriff auf abgelaufene Zertifikate beibehalten werden soll, sodass Benutzer ältere E-Mail-Nachrichten, die mithilfe dieser Zertifikate verschlüsselt wurden, weiterhin öffnen können, wählen Sie die Option **Zertifikatsverlauf einschließen** aus.
8. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind:

- Weisen Sie die Profile Benutzerkonten und Benutzergruppen zu. Android-Benutzer werden beim Empfang des Profils zur Eingabe eines Kennworts aufgefordert (das Kennwort wird auf dem Bildschirm angezeigt).
- Wenn Geräte Entrust-Client-Zertifikate zur Authentifizierung bei einem Wi-Fi-Netzwerk, VPN oder Mailserver verwenden, verknüpfen Sie das Profil mit Benutzeranmeldeinformationen mit einem Wi-Fi-, VPN- oder E-Mail-Profil.

Geschäfts-verbindungen

Richten Sie Geschäftsverbindungen für Geräte ein, z. B. Verbindungen zu Mailservern, Wi-Fi-Netzwerken und VPNs.

Multiplatform

Geschäftsverbindungen für Geräte einrichten

15

Sie können Profile verwenden, um Geschäftsverbindungen für Geräte in Ihrer Organisation einzurichten und zu verwalten. Geschäftsverbindungen legen fest, wie die Geräte eine Verbindung zu den geschäftlichen Ressourcen in Ihrem Unternehmensnetzwerk aufbauen, z. B. zu Mailservern, Proxy-Servern, Wi-Fi-Netzwerken und VPNs. Sie können Einstellungen für BlackBerry 10-, iOS-, Android- und Windows Phone-Geräte in dem gleichen Profil festlegen und das Profil dann Benutzerkonten, Benutzergruppen oder Gerätegruppen zuweisen.

Schritte zum Einrichten von Geschäftsverbindungen für Geräte

Führen Sie zum Einrichten der Geschäftsverbindungen für Geräte die folgenden Aktionen aus:

Schritt	Aktion
1	Erstellen Sie Konfigurationen, die festlegen, wie die Geräte eine Verbindung zu geschäftlichen Ressourcen aufbauen.
2	Legen Sie ggf. eine Rangfolge für die Profile fest.
3	Weisen Sie Benutzerkonten, Benutzergruppen oder Gerätegruppen Profile zu.

Verwalten von geschäftlichen Verbindungen mithilfe von Profilen

Sie können Geschäftsverbindungen über die in der Bibliothek „Richtlinien und Profile“ verfügbaren Profile verwalten.

Sie können mithilfe der folgenden Profile konfigurieren, wie die Geräte eine Verbindung zu geschäftlichen Ressourcen aufbauen:

Profil	Beschreibung
E-Mail	E-Mail-Profile legen fest, wie Geräte eine Verbindung zum geschäftlichen E-Mail-Server herstellen und E-Mail-Nachrichten und Kalendereinträge mithilfe von Exchange ActiveSync oder IBM Notes Traveler synchronisieren.
IMAP/POP3-E-Mail	Ein IMAP/POP3-E-Mail-Profil legt fest, wie Geräte eine Verbindung mit einem IMAP- bzw. POP3-E-Mail-Server aufbauen und E-Mail-Nachrichten synchronisieren.
Zertifikatsabruf	Ein Zertifikatsabrufprofil legt fest, wie Geräte Zertifikate von LDAP-Servern abrufen.
OCSP	Ein OCSP-Profil legt die OCSP-Responder fest, die von den BlackBerry 10-Geräten verwendet werden können, um den Status der Zertifikate zu überprüfen.
CRL	Ein CRL-Profil legt die CRL-Konfigurationen fest, die die BES12 verwenden können, um den Status der Zertifikate zu überprüfen.
Proxy	Ein Proxy-Profil legt fest, wie die Geräte einen Proxy-Server nutzen, um auf Webdienste im Internet oder auf ein geschäftliches Netzwerk zuzugreifen.
VPN	Ein VPN-Profil legt fest, wie die Geräte eine Verbindung zu einem geschäftlichen VPN aufbauen.
Wi-Fi	Ein Wi-Fi-Profil legt fest, wie die Geräte eine Verbindung zu einem geschäftlichen Wi-Fi-Netzwerk aufbauen.
Enterprise-Konnektivität	Ein Enterprise-Konnektivitäts-Profil legt fest, ob gesicherte Apps auf iOS- und Android-Geräten mit Secure Work Space über BlackBerry Infrastructure eine Verbindung zu einem geschäftlichen Netzwerk herstellen müssen. Geschäftliche Apps auf BlackBerry 10-Geräten verwenden BlackBerry Infrastructure wenn ein geschäftliches VPN oder eine Wi-Fi-Verbindung nicht zur Verfügung steht. Das Profil legt auch fest, ob BlackBerry 10-, KNOX Workspace- und Android for Work-Geräte BlackBerry Secure Connect Plus für sichere Verbindungen mit geschäftlichen Ressourcen hinter der Firewall verwenden können, wenn keine geschäftliche VPN- oder Wi-Fi-Verbindung verfügbar ist. BES12 enthält ein Standardprofil für die Enterprise-Konnektivität.
Einmalige Anmeldung	Ein Profil für die einmalige Anmeldung legt fest, wie die Geräte bei sicheren Domänen automatisch eine Authentifizierung durchführen, nachdem die Benutzer zum ersten Mal ihren Benutzernamen und ihr Kennwort eingegeben haben.

Bewährtes Verfahren: Erstellen von Profilen für Geschäftsverbindungen

Einige Geschäftsverbindungsprofile können ein oder mehrere verknüpfte Profile enthalten. Wenn Sie ein angeschlossenes Profil festlegen, verknüpfen Sie ein vorhandenes Profil mit einem Geschäftsverbindungsprofil, und die Geräte müssen das angeschlossene Profil verwenden, wenn sie das Verbindungsprofil nutzen.

Beachten Sie die folgenden Richtlinien:

- Legen Sie fest, welche geschäftlichen Verbindungen für die Geräte in Ihrer Organisation erforderlich sind.
- Erstellen Sie Profile, die Sie mit anderen Profilen verknüpfen können, bevor Sie die Verbindungsprofile erstellen, die diese Profile nutzen.
- Verwenden Sie wenn möglich Variablen.

Sie können Zertifikatsprofile und Proxyprofile diversen Profilen für geschäftliche Verbindungen zuweisen. Profile müssen in der folgenden Reihenfolge erstellt werden:

1. Zertifikatsprofile
2. Proxy-Profile
3. Profile für geschäftliche Verbindungen, z. B. E-Mail, VPN und Wi-Fi

Wenn Sie beispielsweise zuerst ein Wi-Fi-Profil erstellen, können Sie bei der Erstellung eines Proxy-Profils dieses nicht mit dem Wi-Fi-Profil verknüpfen. Nach dem Erstellen eines Proxy-Profils müssen Sie das Wi-Fi-Profil ändern, um es mit dem Proxy-Profil verknüpfen zu können.

Verwandte Informationen
Verwenden von Variablen in Profilen, auf Seite 64

Einrichten des geschäftlichen E-Mail-Kontos für Geräte

Sie können E-Mail-Profile verwenden, um festzulegen, wie Geräte eine Verbindung zum Mailserver Ihrer Organisation herstellen und E-Mail-Nachrichten und Terminplanerdaten mithilfe von Exchange ActiveSync oder IBM Notes Traveler synchronisieren.

Wenn Sie Exchange ActiveSync verwenden möchten, sollten Sie Folgendes beachten:

- Zur Erhöhung der E-Mail-Sicherheit können Sie S/MIME für iOS- und Android-Geräte aktivieren. Sie können S/MIME oder PGP für BlackBerry 10-Geräte aktivieren. PGP wird von BlackBerry 10 OS Version 10.3.1 und höher unterstützt.
- Wenn Sie S/MIME aktivieren, können Sie zusätzliche Profile verwenden, um S/MIME-Zertifikate automatisch mit den Geräten abzurufen und den Zertifikatstatus zu prüfen.

Wenn Sie Notes Traveler verwenden möchten, sollten Sie Folgendes beachten:

- Um Notes Traveler mit iOS- oder Android-Geräten zu nutzen, müssen Sie Secure Work Space aktivieren.

- Um Notes Traveler mit BlackBerry 10- oder Windows Phone-Geräten zu nutzen, müssen Sie die entsprechenden Einstellungen im E-Mail-Profil konfigurieren.
- Die Synchronisierung von Aufgabendaten wird nur auf BlackBerry 10-Geräten unterstützt. Sie nutzt das SyncML-Kommunikationsprotokoll auf dem Notes Traveler-Server.
- Zur Erhöhung der E-Mail-Sicherheit auf BlackBerry 10-Geräten wird nur die IBM Notes-Verschlüsselung unterstützt (nicht aber S/MIME).

Mithilfe von IMAP/POP3-E-Mail-Profilen können Sie auch festlegen, wie iOS-, Android- und Windows Phone-Geräte eine Verbindung zu IMAP- oder POP3-Mailserver herstellen und E-Mail-Nachrichten synchronisieren. Geräte, die für die Verwendung von KNOX MDM aktiviert wurden, unterstützen weder IMAP noch POP3.

Erstellen eines E-Mail-Profils

Die erforderlichen Profileinstellungen sind je nach Gerätetyp unterschiedlich und hängen von dem in der Umgebung Ihrer Organisation genutzten E-Mail-Server ab.

Bevor Sie beginnen:

- Wenn Sie die zertifikatbasierte Authentifizierung zwischen Geräten und Ihrem E-Mail-Server verwenden, müssen Sie ein Profil für ein Zertifizierungsstellenzertifikat erstellen und Benutzern zuweisen und sicherstellen, dass die Geräte über ein vertrauenswürdiges Clientzertifikat verfügen. Sie können ein Zertifikatprofil erstellen und es dem E-Mail-Profil zuweisen, um Clientzertifikate an Geräte zu senden. BlackBerry 10-Geräte unterstützen SCEP-Profile und Profile für Benutzeranmeldeinformationen. iOS-Geräte mit MDM-Steuerelemente-Aktivierung und Android-Geräte mit KNOX Workspace unterstützen Profile für SCEP, Benutzeranmeldeinformationen und freigegebene Zertifikate. iOS- und Android-Geräte mit Secure Work Space unterstützen SCEP-Profile. Android for Work-Geräte unterstützen Profile für Benutzeranmeldeinformationen und für freigegebene Zertifikate.
- Damit ein E-Mail-Profil automatisch auf Android-Geräte angewendet werden kann, müssen die Geräte eines der nachfolgend aufgeführten Kriterien erfüllen. Wenn das Gerät keines dieser Kriterien erfüllt, sendet BES12 das E-Mail-Profil zwar an Android-Geräte, aber der Benutzer muss die Verbindung zum E-Mailserver manuell konfigurieren:
    - Geräte mit Secure Work Space
    - Android for Work-Geräte
    - Samsung-Geräte (einschließlich Samsung KNOX), mit Android 4.4.2 und höher
    - Motorola-Geräte
    - Geräte, auf denen die TouchDown-App installiert ist. Weitere Informationen zur TouchDown-App finden Sie unter nitrodesk.com.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf + neben **E-Mail**.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein.

4. Geben Sie bei Bedarf den Domänennamen des Mailservers an. Wenn das Profil für mehrere Benutzer gilt, die sich in unterschiedlichen Microsoft Active Directory-Domänen befinden können, können Sie die Variable **%UserDomain%** verwenden.
5. Führen Sie im Feld **E-Mail-Adresse** eine der folgenden Aktionen aus:
    - Wenn Sie das Profil für einen Benutzer erstellen, geben Sie die E-Mail-Adresse des Benutzers ein.
    - Wenn Sie das Profil für mehrere Benutzer erstellen, geben Sie **%UserEmailAddress%** ein.
6. Geben Sie den Hostnamen oder die IP-Adresse Mailservers ein.
7. Führen Sie im Feld **Benutzername** eine der folgenden Aktionen aus:
    - Wenn Sie das Profil für einen Benutzer erstellen, geben Sie den Benutzernamen ein.
    - Wenn Sie das Profil für mehrere Benutzer erstellen, geben Sie **%UserName%** ein.
    - Wenn Sie das Profil für mehrere Benutzer in einer IBM Notes Traveler-Umgebung erstellen, geben Sie **%UserDisplayName%** ein.
8. Wenn Sie automatisches Gatekeeping nutzen, klicken Sie auf **Server auswählen**, wählen Sie die entsprechenden Microsoft Exchange-Server aus der Liste der verfügbaren Server aus, und klicken Sie dann auf **Speichern**.
9. Klicken Sie auf die Registerkarte für jeden Gerätetyp in Ihrer Organisation, und konfigurieren Sie die entsprechenden Werte für jede Profileinstellung.
10. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Wenn Sie mehr als ein E-Mail-Profil erstellen möchten, weisen Sie den Profilen eine Rangordnung zu.

Verwandte Informationen
E-Mail-Profileinstellungen, auf Seite 330
Integration von BES12 mit der Entrust-Software Ihrer Organisation, auf Seite 76

Erstellen eines IMAP/POP3-E-Mail-Profils

Die erforderlichen Profileinstellungen sind je nach Gerätetyp unterschiedlich und hängen von den Einstellungen ab, die Sie ausgewählt haben.

Hinweis: BES12 sendet das E-Mail-Profil an Android-Geräte; der Benutzer muss die Verbindung zum Mailserver jedoch manuell konfigurieren.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf + neben **IMAP/POP3-E-Mail**.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
4. Geben Sie im Feld **E-Mail-Typ** den Typ des E-Mail-Protokolls ein.
5. Führen Sie im Feld **E-Mail-Adresse** eine der folgenden Aktionen aus:
    - Wenn Sie das Profil für einen Benutzer erstellen, geben Sie die E-Mail-Adresse des Benutzers ein.

- Wenn Sie das Profil für mehrere Benutzer erstellen, geben Sie **%UserEmailAddress%** ein.

6. Geben Sie im Abschnitt **Einstellungen für eingehende E-Mail-Nachrichten** den Hostnamen oder die IP-Adresse des Mailservers ein, um E-Mail-Nachrichten zu empfangen.
7. Geben Sie ggf. den Port für den Empfang von E-Mail-Nachrichten ein.
8. Führen Sie im Feld **Benutzername** eine der folgenden Aktionen aus:
   - Wenn Sie das Profil für einen Benutzer erstellen, geben Sie den Benutzernamen ein.
   - Wenn Sie das Profil für mehrere Benutzer erstellen, geben Sie **%UserName%** ein.
9. Geben Sie im Abschnitt **Einstellungen für ausgehende E-Mail-Nachrichten** den Hostnamen oder die IP-Adresse des Mailservers ein, um E-Mail-Nachrichten zu senden.
10. Geben Sie ggf. den Port zum Senden von E-Mail-Nachrichten ein.
11. Wählen Sie ggf. die Option **Authentifizierung für ausgehende E-Mail-Nachrichten erforderlich** aus, und geben Sie die Anmeldeinformationen zum Senden von E-Mail-Nachrichten ein.
12. Klicken Sie auf die Registerkarte für jeden Gerätetyp in Ihrer Organisation, und konfigurieren Sie die entsprechenden Werte für jede Profileinstellung.
13. Klicken Sie auf **Hinzufügen**.

Erweitern der E-Mail-Sicherheit mithilfe von S/MIME

Sie können die E-Mail-Sicherheit für die Benutzer von BlackBerry 10-, iOS- und Android-Geräten durch Aktivierung von S/MIME erhöhen. Mit S/MIME steht ein Standardverfahren zur Verschlüsselung und zum Signieren von E-Mail-Nachrichten zur Verfügung. Die Benutzer können E-Mail-Nachrichten mit dem S/MIME-Schutz signieren, verschlüsseln oder signieren und verschlüsseln, wenn sie E-Mail-Nachrichten von einem geschäftlichen E-Mail-Konto senden, das S/MIME-geschützte Nachrichten auf Geräten unterstützt. S/MIME kann für persönliche E-Mail-Adressen nicht aktiviert werden.

Die Benutzer können die S/MIME-Zertifikate der Empfänger auf ihren Geräten speichern. Benutzer können ihre privaten Schlüssel auf ihren Geräten oder einer Smartcard speichern.

Sie können S/MIME für Benutzer in einem E-Mail-Profil aktivieren. Sie können die Benutzer von BlackBerry 10-Geräten zum Einsatz von S/MIME zwingen, aber nicht die Benutzer von iOS- oder Android-Geräten. Wenn die Nutzung von S/MIME optional ist, kann ein Benutzer S/MIME auf dem Gerät aktivieren und angeben, ob E-Mail-Nachrichten verschlüsselt, signiert oder verschlüsselt und signiert werden sollen.

Die S/MIME-Einstellungen haben Vorrang vor den PGP-Einstellungen. Wenn die S/MIME-Unterstützung auf „Erforderlich“ gesetzt wird, werden die PGP-Einstellungen ignoriert.

Weitere Informationen zu S/MIME finden Sie in der Dokumentation zur Sicherheit.

Abrufen von S/MIME-Zertifikaten

Sie können Zertifikatsabrufprofile verwenden, um den Geräten zu ermöglichen, die S/MIME-Zertifikate von LDAP-Servern zu suchen und abzurufen. Wenn sich ein erforderliches S/MIME-Zertifikat nicht bereits im Zertifikatspeicher des Geräts befindet, wird es von dem Gerät automatisch vom Server abgerufen und importiert.

Gerätetyp	Beschreibung
BlackBerry 10	Die Geräte durchsuchen jeden LDAP-Zertifikatserver, den Sie im Profil festlegen, und rufen das S/MIME-Zertifikat ab. Wenn mehr als ein S/MIME-Zertifikat vorliegt und ein Gerät nicht ermitteln kann, welches zu bevorzugen ist, zeigt das Gerät alle S/MIME-Zertifikate an, sodass der Benutzer auswählen kann, welches davon verwendet werden soll. Sie können verlangen, dass die Geräte entweder die einfache Authentifizierung oder Kerberos-Authentifizierung verwenden, um sich bei LDAP-Zertifikatservern zu authentifizieren. Wenn Sie verlangen, dass die Geräte eine einfache Authentifizierung verwenden, können Sie die erforderlichen Authentifizierungs-Anmeldeinformationen in die Zertifikatsabrufprofile einbinden, sodass sich die Geräte automatisch bei den LDAP-Zertifikatservern authentifizieren können. Wenn Sie verlangen, dass die Geräte eine Kerberos-Authentifizierung verwenden, können Sie die erforderlichen Authentifizierungs-Anmeldeinformationen in die Zertifikatsabrufprofile einbinden, sodass sich die Geräte, auf denen BlackBerry 10 OS ab Version 10.3.1 ausgeführt wird, automatisch bei den LDAP-Zertifikatservern authentifizieren können. Andernfalls fordert das Gerät bei der ersten Authentifizierung bei einem LDAP-Zertifikatserver den Benutzer zur Eingabe der erforderlichen Anmeldedaten für die Authentifizierung auf. Bei Geräten, auf denen BlackBerry 10 OS Version 10.2.1 bis 10.3 ausgeführt wird, fordert das Gerät bei der ersten Authentifizierung bei einem LDAP-Zertifikatserver den Benutzer zur Eingabe der erforderlichen Anmeldedaten für die Authentifizierung auf.
iOS und Android	Die Geräte durchsuchen den LDAP-Zertifikatserver, den Sie im Profil festlegen, und rufen das S/MIME-Zertifikat ab. Bei der Authentifizierung der Geräte beim LDAP-Zertifikatserver wird die Kennwortauthentifizierung verwendet. Sie geben das erforderliche Kennwort im Zertifikatsabrufprofil an, sodass Geräte eine automatische Authentifizierung beim LDAP-Zertifikatserver durchführen können.

Wenn Sie kein Zertifikatsabrufprofil erstellen und es den Benutzerkonten, Benutzergruppen oder Gerätegruppen zuweisen, müssen die Benutzer die S/MIME-Zertifikate aus dem Anhang einer geschäftlichen E-Mail oder von einem Computer manuell importieren.

Erstellen eines Zertifikatsabrufprofils

Bevor Sie beginnen: Damit die Geräte den LDAP-Zertifikatservern vertrauen können, wenn sie sichere Verbindungen herstellen, müssen Sie die Zertifizierungsstellenzertifikate ggf. an die Geräte versenden. Falls erforderlich, erstellen Sie Profile für Zertifizierungsstellenzertifikate, und weisen sie den Benutzerkonten, Benutzergruppen oder Gerätegruppen zu.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf + neben **Zertifikatsabruf**.
3. Geben Sie einen Namen und eine Beschreibung für das Profil des Zertifizierungsstellenzertifikats ein.
4. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Verwenden von LDAP für BlackBerry 10	1. Klicken Sie in der Tabelle auf + . 2. Geben Sie im Feld **Dienst-URL** den FQDN eines LDAP-Zertifikatservers in folgendem Format ein: ldap://<*fqdn*>:<*port*>. (Beispiel: ldap://server01.beispiel.com:389). 3. Geben Sie im Feld **Basissuche** die Basis-DN ein, die bei der Suche der LDAP-Zertifikatserver der Ausgangspunkt ist. 4. Führen Sie in der Dropdown-Liste **Suchbereich** eine der folgenden Aktionen aus: • Um nur das Basisobjekt (Basis-DN) zu suchen, klicken Sie auf **Basis**. Diese Option ist der Standardwert. • Um nicht das Basisobjekt, sondern eine Ebene unter dem Basisobjekt zu suchen, klicken Sie auf **Eine Ebene**. • Um das Basisobjekt und alle Ebenen darunter zu suchen, klicken Sie auf **Unterstruktur**. • Um alle Ebenen unter dem Basisobjekt zu suchen, aber nicht das Basisobjekt selbst, klicken Sie auf **Untergeordnet**. 5. Wenn eine Authentifizierung erforderlich ist, führen Sie die folgenden Aktionen aus: a Klicken Sie in der Dropdown-Liste **Authentifizierungstyp** auf **Einfach** oder **Kerberos**. b Geben Sie im Feld **LDAP-Benutzer-ID** die DN eines Kontos ein, das Suchberechtigungen auf dem LDAP-Zertifikatserver hat (zum Beispiel cn=admin, dc=beispiel, dc=com). c Geben Sie im Feld **LDAP-Kennwort** das Kennwort für das Konto ein, das Suchberechtigungen auf dem LDAP-Zertifikatserver hat.

Aufgabe	Schritte
	6. Aktivieren Sie ggf. das Kontrollkästchen **Sichere Verbindung verwenden**. 7. Geben Sie im Feld **Verbindungs-Timeout** die Zeit in Sekunden ein, die das Gerät auf eine Antwort des LDAP-Zertifikatservers wartet. 8. Klicken Sie auf **Hinzufügen**. 9. Wiederholen Sie die Schritte 4.2 bis 4.8 für jeden LDAP-Zertifikatserver.
Verwenden von LDAP für iOS- und Android-Geräte	1. Wählen **LDAP verwenden** aus. 2. Geben Sie im Feld **Dienst-URL** den FQDN eines LDAP-Zertifikatservers in folgendem Format ein: ldap://<*fqdn*>:<*port*>. (Beispiel: ldap://server01.beispiel.com:389) 3. Geben Sie im Feld **Basis-DN** die Stamm-DN in dem Verzeichnis ein, wo die Suche durch das Gerät stattfinden soll. (Beispiel: ou=users, de=beispiel, dc=com) 4. Geben Sie im Feld **Verbindungs-DN** die DN eines Kontos ein, das Suchberechtigungen auf dem LDAP-Zertifikatserver hat. (Beispiel: cn=admin,dc=beispiel,dc=com). 5. Geben Sie im Feld **LDAP-Kennwort** das Kennwort für die Verbindungs-DN ein. 6. Aktivieren Sie ggf. das Kontrollkästchen **Sichere Verbindung verwenden**.
Verwendung von Exchange ActiveSync für iOS- und Android-Geräte	1. Wählen Sie **Exchange ActiveSync verwenden** aus.

5. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind:

- Um BlackBerry 10-Geräten zu erlauben, den Zertifikatstatus zu überprüfen, erstellen Sie ein OCSP- oder CRL-Profil.
- Wenn Sie mehrere Zertifikatsabrufprofile erstellen, weisen Sie ihnen eine Rangordnung zu.

Ermitteln des Status von S/MIME-Zertifikaten auf Geräten

Sie können OCSP- und CRL-Profile verwenden, um den BlackBerry 10-Geräten zu erlauben, den Status der S/MIME-Zertifikate zu überprüfen. Sie können den Benutzerkonten, den Benutzergruppen oder den Gerätegruppen ein OCSP-Profil und ein CRL-Profil zuweisen.

BlackBerry 10-Geräte durchsuchen jeden OCSP-Responder, den Sie im OCSP-Profil vorgeben, und rufen den Status des S/MIME-Zertifikats ab. Geräte, auf denen BlackBerry 10 OS Version ab 10.3.1 ausgeführt wird, können Zertifikat-Statusabfragen an BES12 senden, und Sie können CRL-Profile zur Konfiguration von BES12 verwenden, um den Status der S/MIME-Zertifikate mit HTTP, HTTPS oder LDAP zu suchen.

Wenn Sie Exchange ActiveSync für den Zertifikatabruf verwenden, verwenden iOS- und Android-Geräte Exchange ActiveSync, um den Status von S/MIME-Zertifikaten zu prüfen. Wenn Sie LDAP für den Zertifikatabruf verwenden, verwenden iOS- und Android-Geräte OCSP, um den Status von Zertifikaten zu prüfen. iOS- und Android-Geräte unterstützen keine OCSP-Profile. Die Geräte prüfen den OCSP-Responder innerhalb des Zertifikats.

Weitere Informationen zu Zertifikatstatusanzeigen finden Sie im Benutzerhandbuch im Abschnitt zu den Symbolen für sichere E-Mail.

Erstellen eines OCSP-Profils

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf + neben **OCSP**.
3. Geben Sie einen Namen und eine Beschreibung für das OCSP-Profil ein.
4. Führen Sie folgende Aktionen aus:
   a. Klicken Sie in der Tabelle auf + .
   b. Geben Sie im Feld **Dienst-URL** die Webadresse eines OCSP-Responders ein.
   c. Geben Sie im Feld **Verbindungs-Timeout** die Zeit in Sekunden ein, die das Gerät auf eine OCSP-Antwort wartet.
   d. Klicken Sie auf **Hinzufügen**.
5. Wiederholen Sie Schritt 4 für jeden OCSP-Responder.
6. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Wenn Sie mehrere OCSP-Profile erstellen, weisen Sie ihnen eine Rangordnung zu.

Erstellen eines CRL-Profils

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf + neben **CRL**.
3. Geben Sie einen Namen und eine Beschreibung für das CRL-Profil ein.
4. Damit die Geräte die Responder-URLs verwenden können, die im Zertifikat definiert sind, aktivieren Sie das Kontrollkästchen **Zertifikaterweiterungen des Responders verwenden**.
5. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Festlegen einer HTTP CRL-Konfiguration	1. Klicken Sie im Abschnitt **HTTP für CRL** auf +. 2. Geben Sie einen Namen und eine Beschreibung für die HTTP CRL-Konfiguration ein. 3. Geben Sie im Feld **Dienst-URL** die Webadresse eines HTTP- oder HTTPS-Servers ein.

Aufgabe	Schritte
	4. Klicken Sie auf **Hinzufügen**. 5. Wiederholen Sie die Schritte 1 bis 4 für jeden HTTP- oder HTTPS-Server.
Festlegen einer LDAP CRL-Konfiguration	1. Klicken Sie im Abschnitt **LDAP für CRL** auf +. 2. Geben Sie einen Namen und eine Beschreibung für die LDAP CRL-Konfiguration ein. 3. Geben Sie im Feld **Dienst-URL** den FQDN eines LDAP-Servers gemäß dem folgenden Format ein: ldap://<*fqdn*>:<*port*> (zum Beispiel ldap://server01.example.com:389). Um sichere Verbindungen herzustellen, verwenden Sie das Format ldaps://<*fqdn*>:<*port*>. 4. Geben Sie im Feld **Basissuche** die Basis-DN ein, die bei der Suche der LDAP-Server der Ausgangspunkt ist. 5. Aktivieren Sie ggf. das Kontrollkästchen **Sichere Verbindung verwenden**. 6. Geben Sie im Feld **LDAP-Benutzer-ID** die DN eines Kontos ein, der Suchberechtigungen auf dem LDAP-Server hat (zum Beispiel cn=admin,dc=example,dc=com). 7. Geben Sie im Feld **LDAP-Kennwort** das Kennwort für das Konto ein, das Suchberechtigungen auf dem LDAP-Server besitzt. 8. Klicken Sie auf **Hinzufügen**. 9. Wiederholen Sie die Schritte 1 bis 8 für jeden LDAP-Server.

6. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Wenn Sie mehrere CRL-Profile erstellen, weisen Sie ihnen eine Rangordnung zu.

Erweitern der E-Mail-Sicherheit mit PGP

Bei Geräten mit einer BlackBerry 10 OS Version ab 10.3.1 können Sie die E-Mail-Sicherheit für Gerätebenutzer erweitern, indem Sie PGP aktivieren. PGP schützt E-Mail-Nachrichten auf Geräten mit dem OpenPGP-Format. Benutzer können E-Mail-Nachrichten mit dem PGP-Schutz signieren, verschlüsseln oder signieren und verschlüsseln, sofern sie eine geschäftliche E-Mail-Adresse verwenden. PGP kann nicht für persönliche E-Mail-Adressen verwendet werden.

Sie können PGP für Benutzer in einem E-Mail-Profil aktivieren. Sie können BlackBerry 10-Gerätebenutzer zwingen, PGP zu verwenden, die Nutzung von PGP untersagen oder ihnen die Nutzung freistellen. Wenn die Nutzung von PGP optional ist (Standardeinstellung), kann ein Benutzer PGP auf dem Gerät aktivieren und angeben, ob E-Mail-Nachrichten verschlüsselt, signiert oder verschlüsselt und signiert werden sollen.

Um E-Mail-Nachrichten zu signieren und zu verschlüsseln, müssen Benutzer PGP-Schlüssel für jeden Empfänger auf ihren Geräten speichern. Benutzer können PGP-Schlüssel speichern, indem sie die Dateien aus einer geschäftlichen E-Mail-Nachricht importieren.

Sie können PGP mit den entsprechenden E-Mail-Profileinstellungen konfigurieren.

Weitere Informationen zu PGP finden Sie in der Dokumentation zur Sicherheit.

Verwandte Informationen

BlackBerry 10: E-Mail-Profileinstellungen, auf Seite 331

Erzwingen von sicherer E-Mail mithilfe der Nachrichtenklassifizierung

Die Nachrichtenklassifizierung ermöglicht es Ihrem Unternehmen, auf BlackBerry 10-Geräten sichere E-Mail-Richtlinien festzulegen und durchzusetzen sowie visuelle Markierungen zu E-Mail-Nachrichten hinzuzufügen. Sie können BES12 verwenden, um Benutzern von BlackBerry 10Geräten die gleichen Optionen zur Nachrichtenklassifizierung zu bieten, die ihnen auch bei den E-Mail-Anwendungen auf ihrem Computer zur Verfügung stehen. Sie können die folgenden Regeln für ausgehende Nachrichten definieren, basierend auf den Nachrichtenklassifizierungen:

- Ein Etikett hinzufügen, um die Nachrichtenklassifizierung zu markieren (z. B. vertraulich)
- Eine optische Markierung am Ende der Betreffzeile hinzufügen (z. B. [C])
- Text am Anfang oder am Ende des E-Mail-Textkörpers hinzufügen (z. B. "Diese Nachricht wurde als vertraulich eingestuft")
- S/MIME oder PGP-Optionen einstellen (z. B. signieren und verschlüsseln)
- Eine Standardklassifizierung einstellen

Auf Geräten, auf denen BlackBerry 10 OS-Version 10.3.1 und höher ausgeführt wird, können Sie mithilfe der Nachrichtenklassifizierung festlegen, dass Benutzer E-Mail-Nachrichten signieren, verschlüsseln oder signieren und verschlüsseln müssen oder visuelle Markierungen zu E-Mail-Nachrichten, die sie von ihren Geräten senden, hinzufügen. Mithilfe von E-Mail-Profilen können Sie Konfigurationsdateien zur Nachrichtenklassifizierung (mit der Dateierweiterung .json) angeben, die an die Geräte der Benutzer gesendet werden. Wenn Benutzer E-Mail-Nachrichten beantworten, für die eine Nachrichtenklassifizierung festgelegt wurde, oder sichere E-Mail-Nachrichten erstellen, bestimmt die Konfiguration der Nachrichtenklassifizierung, welche Klassifizierungsregeln von den Geräten bei ausgehenden Nachrichten erzwungen werden müssen.

Die Nachrichtenschutzoptionen auf einem Gerät sind auf die Arten der Verschlüsselung und digitalen Signatur beschränkt, die auf dem Gerät zugelassen sind. Wenn ein Benutzer eine Nachrichtenklassifizierung für eine E-Mail-Nachricht auf einem Gerät anwendet, muss der Benutzer eine Nachrichtenschutzart auswählen, die die betreffende Nachrichtenklassifizierung zulässt, oder den Standardschutz akzeptieren. Wenn ein Benutzer eine Nachrichtenklassifizierung auswählt, die eine Signatur und/oder Verschlüsselung der E-Mail-Nachricht erfordert, und auf dem Gerät S/MIME oder PGP nicht konfiguriert ist, kann der Benutzer die E-Mail-Nachricht nicht senden.

Die S/MIME- und PGP-Einstellungen haben Vorrang vor der Nachrichtenklassifizierung. Benutzer können die Stufe der Nachrichtenklassifizierung auf ihren Geräten anheben, aber nicht absenken. Die Stufen der Nachrichtenklassifizierung werden von Regeln für sichere E-Mails in jeder Klassifizierung festgelegt.

Wenn die Nachrichtenklassifizierung aktiviert ist, können Benutzer keine E-Mail-Nachrichten mithilfe von BlackBerry Assistant von ihren Geräten senden.

Sie können die Nachrichtenklassifizierung mit den entsprechenden E-Mail-Profileinstellungen konfigurieren.

Weitere Informationen über das Erstellen von Konfigurationsdateien zur Nachrichtenklassifizierung finden Sie unter blackberry.com/go/kbhelp im Artikel KB36736.

Verwandte Informationen
BlackBerry 10: E-Mail-Profileinstellungen, auf Seite 331

Einrichten von Proxy-Konfigurationen für Geräte

Mithilfe von Proxy-Profilen können Sie festlegen, wie die Geräte einen Proxy-Server nutzen, um auf Webdienste im Internet oder auf ein geschäftliches Netzwerk zuzugreifen.

Gerät	Zuordnung des Proxy-Profils
BlackBerry 10	Um Proxy-Profile verwenden zu können, müssen Sie sie den von Ihrer Organisation verwendeten Profilen zuordnen, nachfolgend: • Wi-Fi • VPN • Enterprise-Konnektivität
iOS	Um Proxy-Profile verwenden zu können, müssen Sie sie den von Ihrer Organisation verwendeten Profilen zuordnen, nachfolgend: • Wi-Fi • VPN • Enterprise-Konnektivität (wenn Sie Geräte mit Secure Work Space verwalten und die Enterprise-Konnektivität aktiviert ist) Sie können auch den Benutzerkonten, den Benutzergruppen oder den Gerätegruppen ein Proxy-Profil zuweisen. **Hinweis:** Ein Proxy-Profil, das Benutzerkonten, Benutzergruppen oder Gerätegruppen zugewiesen wird, ist nur ein globaler Proxy für überwachte Geräte und hat Vorrang vor einem Proxy-Profil, das mit einem VPN- oder Wi-Fi-Profil verknüpft ist. Wenn die Enterprise-Konnektivität aktiviert ist, nutzen die gesicherten Apps die Proxy-Einstellungen, die mit einem Enterprise-Konnektivitätsprofil verknüpft sind, während geschäftliche und persönliche Apps die globalen Proxy-Einstellungen verwenden. Andernfalls verwenden die überwachten Geräte die globalen Proxy-Einstellungen für alle HTTP-Verbindungen.

Gerät	Zuordnung des Proxy-Profils
Android mit Secure Work Space	Wenn die Enterprise-Konnektivität aktiviert ist, müssen Sie zur Verwendung eines Proxy-Profils dieses mit einem Enterprise-Konnektivitätsprofil verknüpfen.
Android for Work	Zur Verwendung eines Proxyprofils müssen Sie dieses einem Wi-Fi-Profil zuweisen.
Geräte mit Samsung KNOX	Zur Verwendung eines Proxyprofils müssen Sie dieses einem Wi-Fi-Profil zuweisen. Geräte mit Samsung KNOX unterstützen nur eine manuelle Proxy-Konfiguration.

Erstellen eines Proxy-Profils

Wenn Ihre Organisation eine PAC-Datei zur Definition von Proxy-Regeln verwendet, können Sie die PAC-Konfiguration auswählen, um die Einstellungen des Proxy-Servers aus der von Ihnen festgelegten PAC-Datei zu verwenden. Andernfalls können Sie die manuelle Konfiguration auswählen und die Einstellungen des Proxy-Servers direkt im Profil festlegen. Proxy-Profile unterstützen Proxy-Server, die nur eine allgemeine Authentifizierung oder gar keine Authentifizierung verwenden. Bei iOS- und Android- Geräten mit Secure Work Space unterstützen Proxy-Profile, die Sie Enterprise-Konnektivitätsprofilen zuordnen, die Proxy-Server, die eine allgemeine Authentifizierung, NTLM oder gar keine Authentifizierung verwenden.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf + neben **Proxy**.
3. Geben Sie einen Namen und eine Beschreibung für das Proxy-Profil ein.
4. Klicken Sie auf die Registerkarte eines Gerätetyps.
5. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Festlegen der Einstellungen für die PAC-Konfiguration	1. Vergewissern Sie sich, dass in der Dropdown-Liste **Typ** die Option **PAC-Konfiguration** ausgewählt ist. 2. Geben Sie im Feld **PAC-URL** die URL für den Webserver an, der die PAC-Datei hostet, sowie den PAC-Dateinamen (zum Beispiel http://www.example.com/PACfile.pac). 3. Führen Sie auf der Registerkarte **BlackBerry** die folgenden Aktionen aus: a Wenn Ihre Organisation erfordert, dass Benutzer einen Benutzernamen und ein Kennwort für die Verbindung zum Proxy-Server eingeben, und das Profil für mehrere Benutzer gilt, geben Sie im Feld **Benutzername %UserName%** ein. Wenn der Proxy-Server den Domänennamen zur Authentifizierung benötigt, verwenden Sie das Format *<domain>**<username>*.

Aufgabe	Schritte
	b Klicken Sie in der Dropdown-Liste **Benutzerdefinierbar** auf die Proxy-Einstellungen, die die Benutzer von BlackBerry 10-Geräten ändern können. Die Standardeinstellung ist **Schreibgeschützt**.
Festlegen der Einstellungen zur manuellen Konfiguration	1. Klicken Sie in der Dropdown-Liste **Typ** auf **Manuelle Konfiguration**. 2. Geben Sie im Feld **Host** den FQDN oder die IP-Adresse des Proxy-Servers ein. 3. Geben Sie im Feld **Port** die Portnummer des Proxy-Servers ein. 4. Wenn Ihre Organisation erfordert, dass Benutzer einen Benutzernamen und ein Kennwort für die Verbindung zum Proxy-Server eingeben, und das Profil für mehrere Benutzer gilt, geben Sie im Feld **Benutzername %UserName%** ein. Wenn der Proxy-Server den Domänennamen zur Authentifizierung benötigt, verwenden Sie das Format *<domain>\<username>*. 5. Führen Sie auf der Registerkarte **BlackBerry** die folgenden Aktionen aus: a Klicken Sie in der Dropdown-Liste **Benutzerdefinierbar** auf die Proxy-Einstellungen, die die Benutzer von BlackBerry 10-Geräten ändern können. Die Standardeinstellung ist **Schreibgeschützt**. b Optional können Sie eine Liste der Adressen festlegen, auf die die Benutzer über ihre BlackBerry 10-Geräte direkt zugreifen können, ohne dazu den Proxy-Server zu verwenden. Geben Sie im Feld **Ausschlussliste** die Adressen (FQDN oder IP) ein, und trennen Sie die einzelnen Werte in der Liste mit einem Semikolon (;).

6. Wiederholen Sie die Schritte 4 und 5 für jeden Gerätetyp in Ihrer Organisation.
7. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind:

- Verknüpfen Sie das Proxy-Profil mit einem Wi-Fi-, VPN- oder Enterprise-Konnektivitätsprofil.
- Wenn Sie mehr als ein Proxy-Profil erstellen möchten, dann legen Sie eine Rangfolge für die Profile fest. Die von Ihnen festgelegte Reihenfolge gilt nur, wenn Sie den Benutzergruppen oder Gerätegruppen ein Proxy-Profil zuweisen.

Einrichten von geschäftlichen Wi-Fi-Netzwerken für Geräte

Sie können Wi-Fi-Profile verwenden, um festzulegen, wie Geräte eine Verbindung zu geschäftlichen Wi-Fi-Netzwerken hinter der Firewall herstellen. Sie können den Benutzerkonten, den Benutzergruppen oder den Gerätegruppen ein Wi-Fi-Profil zuweisen.

Gerät	App- und Netzwerkverbindungen
BlackBerry 10	Standardmäßig können sowohl geschäftliche als auch persönliche Apps die auf dem Gerät gespeicherten Wi-Fi-Profile verwenden, um eine Verbindung zum Netzwerk Ihrer Organisation herzustellen. Geschäftliche Apps können zum Herstellen einer Verbindung zum Netzwerk Ihrer Organisation auch BlackBerry Infrastructure-Profile verwenden. Wenn die Sicherheitsrichtlinien Ihrer Organisation nicht zulassen, dass persönliche Apps auf das Netzwerk Ihrer Organisation zugreifen, können Sie die Verbindungsoptionen einschränken. Weitere Informationen finden Sie in der Dokumentation zur Sicherheit.
iOS	Die folgenden Apps können die auf dem Gerät gespeicherten Wi-Fi-Profile verwenden, um eine Verbindung zum Netzwerk Ihrer Organisation herzustellen. • Geschäftliche und persönliche Apps • Gesicherte Apps (auf Geräten mit Secure Work Space)
Android	Die folgenden Apps können die auf dem Gerät gespeicherten Wi-Fi-Profile verwenden, um eine Verbindung zum Netzwerk Ihrer Organisation herzustellen. • Geschäftliche und persönliche Apps • Gesicherte Apps (auf Geräten mit Secure Work Space)
Windows Phone	Geschäftliche Apps und persönliche Apps können die auf dem Gerät gespeicherten Wi-Fi-Profile verwenden, um eine Verbindung zum Netzwerk Ihrer Organisation herzustellen.

Erstellen eines Wi-Fi-Profils

Die erforderlichen Profileinstellungen sind je nach Gerätetyp unterschiedlich und hängen vom Wi-Fi-Sicherheitstyp und dem Authentifizierungsprotokoll ab, die Sie ausgewählt haben.

Bevor Sie beginnen:

- Wenn die Geräte eine zertifikatbasierte Authentifizierung für Wi-Fi-Geschäftsverbindungen verwenden, erstellen Sie ein Profil mit Zertifizierungsstellenzertifikat, und weisen Sie es Benutzerkonten, Benutzergruppen oder Gerätegruppen zu. Um Client-Zertifikate an Geräte zu senden, erstellen Sie ein SCEP-Profil, ein Profil für

Benutzeranmeldeinformationen oder ein Profil für ein freigegebenes Zertifikat, das Sie mit dem Wi-Fi-Profil verknüpfen.

- Erstellen Sie für BlackBerry 10, iOS, Android for Work oder Geräte, auf denen Samsung KNOX und ein Proxy-Server für geschäftliche Wi-Fi-Verbindungen verwendet werden, ein Proxy-Profil, das Sie mit dem Wi-Fi-Profil verknüpfen.
- Wenn BlackBerry 10-Geräte ein VPN für geschäftliche Wi-Fi-Verbindungen verwenden, erstellen Sie ein VPN-Profil, das Sie mit dem Wi-Fi-Profil verknüpfen.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf + neben **Wi-Fi**.
3. Geben Sie einen Namen und eine Beschreibung für das Wi-Fi-Profil ein. Diese Informationen werden auf den Geräten angezeigt.
4. Geben Sie im Feld **SSID** den Netzwerknamen eines Wi-Fi-Netzwerks ein.
5. Wenn das Wi-Fi-Netzwerk die SSID nicht sendet, aktivieren Sie das Kontrollkästchen **Verborgenes Netzwerk**.
6. Deaktivieren Sie optional das Kontrollkästchen für alle Gerätetypen, für die Sie das Profil nicht konfigurieren möchten.
7. Führen Sie folgende Aktionen aus:
   a. Klicken Sie auf die Registerkarte eines Gerätetyps.
   b. Konfigurieren Sie die entsprechenden Werte für jede Profileinstellung so, dass sie der Wi-Fi-Konfiguration in Ihrer Organisationsumgebung entsprechen. Wenn Ihre Organisation erfordert, dass Benutzer einen Benutzernamen und ein Kennwort für den Zugriff auf das Wi-Fi-Netzwerk eingeben, und das Profil für mehrere Benutzer gilt, geben Sie im Feld **Benutzername %UserName%** ein.
8. Wiederholen Sie Schritt 7 für jeden Gerätetyp in Ihrer Organisation.
9. Klicken Sie auf **Hinzufügen**.

Verwandte Informationen

Verwalten von Zertifikaten mithilfe von Profilen, auf Seite 70
Wi-Fi-Profileinstellungen, auf Seite 369
Integration von BES12 mit der Entrust-Software Ihrer Organisation, auf Seite 76

Einrichten von geschäftlichen VPNs für Geräte

Sie können mithilfe von VPN-Profilen festlegen, wie BlackBerry 10-, iOS- und KNOX Workspace-Geräte eine Verbindung mit einem geschäftlichen VPN aufbauen. Sie können den Benutzerkonten, den Benutzergruppen oder den Gerätegruppen ein VPN-Profil zuweisen. Bei BlackBerry 10-Geräten können Sie auch ein VPN-Profil mit einem Wi-Fi-Profil verknüpfen.

Zum Herstellen einer Verbindung zu einem geschäftlichen VPN müssen Benutzer von Android- und Windows Phone-Geräten die VPN-Einstellungen auf ihren Geräten manuell konfigurieren.

Gerät	App- und Netzwerkverbindungen
BlackBerry 10	• Standardmäßig können sowohl geschäftliche als auch persönliche Apps die auf dem Gerät gespeicherten VPN-Profile verwenden, um eine Verbindung zum Netzwerk Ihrer Organisation herzustellen. Geschäftliche Apps können zum Herstellen einer Verbindung zum Netzwerk Ihrer Organisation auch BlackBerry Infrastructure-Profile verwenden. Wenn die Sicherheitsrichtlinien Ihrer Organisation nicht zulassen, dass persönliche Apps auf das Netzwerk Ihrer Organisation zugreifen, können Sie die Verbindungsoptionen einschränken. Weitere Informationen finden Sie in der Dokumentation zur Sicherheit.
iOS	• Geschäftliche und private Apps können die auf dem Gerät gespeicherten VPN-Profile verwenden, um eine Verbindung zum Netzwerk Ihrer Organisation herzustellen. Sie können Per App VPN für ein VPN-Profil aktivieren, um das Profil nur auf die festgelegten geschäftlichen Apps anzuwenden. • Bei Geräten mit Secure Work Space nutzen gesicherte Apps standardmäßig die Enterprise-Konnektivität, um eine Verbindung zu Ihrem Unternehmensnetzwerk herzustellen. Sie können die Enterprise-Konnektivität deaktivieren, wenn die gesicherten Apps die auf dem Gerät verfügbaren Verbindungen nutzen sollen.
KNOX Workspace	• Geschäftliche und private Apps können die auf dem Gerät gespeicherten VPN-Profile verwenden, um eine Verbindung zum Netzwerk Ihrer Organisation herzustellen. • Die Benutzer müssen die geeignete VPN-Client-App auf ihrem Gerät installieren, um das VPN-Profil verwenden zu können. Unterstützt werden die VPN-Client-Apps Cisco AnyConnect und Juniper. **Hinweis:** Die Juniper-App unterstützt nur SSL-VPN.

Erstellen eines VPN-Profils

Die erforderlichen Profileinstellungen sind je nach Gerätetyp unterschiedlich und hängen vom VPN-Verbindungstyp und dem Authentifizierungstyp ab, die Sie ausgewählt haben.

Hinweis: Auf einigen Geräten kann das xAuth-Kennwort nicht gespeichert werden. Weitere Informationen finden Sie im Artikel KB30353 unter www.blackberry.com/go/kbhelp.

Bevor Sie beginnen:

- Wenn Geräte die zertifikatbasierte Authentifizierung für geschäftliche VPN-Verbindungen nutzen, erstellen Sie ein Profil mit Zertifizierungsstellenzertifikat, und weisen Sie es Benutzerkonten, Benutzergruppen oder Gerätegruppen zu. Um Client-Zertifikate an Geräte zu senden, erstellen Sie ein SCEP-Profil, ein Profil für

Benutzeranmeldeinformationen oder ein Profil für ein freigegebenes Zertifikat, das Sie mit dem VPN-Profil verknüpfen.

- Wenn Geräte einen Proxy-Server für geschäftliche VPN-Verbindungen verwenden, erstellen Sie ein Proxy-Profil, das Sie mit dem VPN-Profil verknüpfen.
- Fügen Sie für KNOX Workspace-Geräte die geeignete VPN-Client-App der App-Liste hinzu, und weisen Sie sie Benutzerkonten, Benutzergruppen oder Gerätegruppen zu. Als VPN-Client-Apps werden Cisco AnyConnect und Juniper unterstützt.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf + neben **VPN**.
3. Geben Sie einen Namen und eine Beschreibung für das VPN-Profil ein. Diese Informationen werden auf den Geräten angezeigt.
4. Deaktivieren Sie optional das Kontrollkästchen für alle Gerätetypen, für die Sie das Profil nicht konfigurieren möchten.
5. Führen Sie folgende Aktionen aus:
   a. Klicken Sie auf die Registerkarte eines Gerätetyps.
   b. Konfigurieren Sie die entsprechenden Werte für jede Profileinstellung so, dass sie der VPN-Konfiguration in Ihrer Organisationsumgebung entsprechen. Wenn Ihre Organisation erfordert, dass Benutzer einen Benutzernamen und ein Kennwort für den Zugriff auf das VPN-Netzwerk eingeben, und das Profil für mehrere Benutzer gilt, geben Sie im Feld **Benutzername %UserName%** ein.
6. Wiederholen Sie Schritt 5 für jeden Gerätetyp in Ihrer Organisation.
7. Klicken Sie auf **Hinzufügen**.

Verwandte Informationen

Verwalten von Zertifikaten mithilfe von Profilen, auf Seite 70
VPN-Profileinstellungen, auf Seite 391
Integration von BES12 mit der Entrust-Software Ihrer Organisation, auf Seite 76

Aktivieren von „VPN bei Bedarf“ für Geräte mit iOS

Mit „VPN bei Bedarf“ können Sie festlegen, ob ein iOS-Gerät beim Versuch, eine Verbindung zu einer bestimmten Domäne aufzubauen, automatisch eine Verbindung zu einem VPN aufbaut. Zertifikate, z. B. SCEP- oder freigegebene Zertifikate, bieten beim Zugriff auf eine bestimmte Domäne Authentifizierungsmöglichkeiten für Benutzergeräte. Sie können die Domäne Ihres Unternehmens beispielsweise so konfigurieren, dass Benutzer mithilfe von „VPN bei Bedarf“ auf Ihre Intranetinhalte zugreifen können.

Verwandte Informationen

iOS: VPN-Profileinstellungen, auf Seite 404

Aktivieren von Per App VPN für iOS-Apps

Sie können Per App VPN verwenden, um zu bestimmen, welche geschäftlichen Apps und gesicherten Apps auf Geräten ein VPN für die Datenübertragung verwenden müssen. Per App VPN trägt zur Senkung der Belastung Ihres Unternehmens-VPN bei, indem nur bestimmter geschäftlicher Datenverkehr für die Verwendung des VPN freigegeben wird (bspw. Zugriff auf Anwendungsserver oder Webseiten hinter der Firewall). Diese Funktion unterstützt auch die Privatsphäre des Benutzers und erhöht die Verbindungsgeschwindigkeit für persönliche Apps, indem der persönliche Datenverkehr nicht über das VPN gesendet wird.

Sie verknüpfen dann Apps mit Per App VPN, indem Apps oder App-Gruppen das VPN-Profil zugewiesen wird.

Verwandte Informationen
iOS: VPN-Profileinstellungen, auf Seite 404

So wählt BES12 die Per App VPN-Einstellungen für die Zuweisung aus

Einer App oder einer App-Gruppe kann nur ein VPN-Profil zugewiesen werden. BES12 verwendet die folgenden Regeln, um zu bestimmen, welche Per App VPN-Einstellungen einer App zugewiesen werden:

- Per App VPN-Einstellungen, die direkt mit einer App verknüpft sind, haben Vorrang vor Per App VPN-Einstellungen, die indirekt durch eine App-Gruppe verknüpft sind.
- Per App VPN-Einstellungen, die direkt mit einem Benutzer verknüpft sind, haben Vorrang vor Per App VPN-Einstellungen, die indirekt durch eine Benutzergruppe verknüpft sind.
- Per App VPN-Einstellungen, die mit einer benötigten App verknüpft sind, haben Vorrang vor Per App VPN-Einstellungen, die einer optionalen Instanz der gleichen App zugewiesen sind.
- Per App VPN-Einstellungen, die mit dem Benutzergruppennamen verknüpft sind, der weiter oben in der alphabetischen Liste angezeigt wird, haben Vorrang, wenn die folgenden Bedingungen erfüllt werden:
    - Eine App ist mehreren Benutzergruppen zugewiesen
    - Die gleiche App wird in den Benutzergruppen angezeigt
    - Die App wird auf die gleiche Art zugewiesen, entweder als einzelne App oder als App-Gruppe
    - Die App hat in allen Zuweisungen die gleiche Verfügbarkeit, entweder erforderlich oder optional

  Beispielsweise ist Cisco WebEx Meetings den Benutzergruppen Entwicklung und Marketing als optionale App zugewiesen. Ist ein Benutzer in beiden Gruppen vorhanden, werden die Per App VPN-Einstellungen für die Entwicklungsgruppe auf die WebEx Meetings-App für diesen Benutzer angewendet.

Wenn das Per App VPN-Profil einer Gerätegruppe zugewiesen ist, hat es für alle Geräte, die dieser Gerätegruppe angehören, Vorrang vor dem Per App VPN-Profil, das dem Benutzerkonto zugewiesen ist.

Einrichten von Enterprise-Konnektivität für Geräte

Mithilfe eines Enterprise-Konnektivitäts-Profils können Sie steuern, wie Apps auf BlackBerry 10-Geräten und iOS- und Android-Geräten mit Secure Work Space eine Verbindung mit den Ressourcen Ihres Unternehmens herstellen. Mit der Enterprise-Konnektivität vermeiden Sie, dass innerhalb der Firewall Ihrer Organisation eine direkte Verbindung mit dem Internet für die Geräteverwaltung und Drittanbieteranwendungen, wie etwa den Mailserver, die Zertifizierungsstelle und andere Web- oder Inhaltsserver, geöffnet wird. Die Enterprise-Konnektivität sendet den gesamten Datenverkehr über die BlackBerry Infrastructure an BES12.

Enterprise-Konnektivitäts-Profile dienen überdies zum Aktivieren von BlackBerry Secure Connect Plus für BlackBerry 10- KNOX Workspace- und Android for Work-Geräte. Weitere Informationen zu BlackBerry Secure Connect Plus finden Sie unter „Verwenden von BlackBerry Secure Connect Plus für sichere Verbindungen mit geschäftlichen Ressourcen“.

Wenn Sie einem Benutzer oder einer Gruppe kein Profil für die Enterprise-Konnektivität zuweisen, wird das Standardprofil für die Enterprise-Konnektivität zugewiesen. Enterprise-Konnektivität und BlackBerry Secure Connect Plus werden für alle unterstützten Geräte im Standardprofil für die Enterprise-Konnektivität aktiviert. Sie können das Standardprofil für die Enterprise-Konnektivität bearbeiten, aber Sie können es nicht löschen.

Wenn die Enterprise-Konnektivität nicht aktiviert ist, greifen Apps auf iOS- oder Android-Geräten mit Secure Work Space über das interne Wi-Fi-Netzwerk oder eine auf dem Gerät konfigurierte VPN-Verbindung auf Ihre Organisationsressourcen zu.

Für BlackBerry 10-Geräte ist die Enterprise-Konnektivität immer aktiviert. Diese Geräte wählen den effektivsten Pfad basierend auf der Netzwerkverfügbarkeit.

Sie können jedem Gerätetyp ein Proxy-Profil zuweisen, für das Sie Enterprise-Konnektivität aktiviert haben.

Erstellen eines Enterprise-Konnektivitäts-Profils

BES12 weist allen Benutzern standardmäßig das Standardprofil für die Enterprise-Konnektivität zu. Sie können das Standardprofil bearbeiten oder neue Enterprise-Konnektivitäts-Profile erstellen. Die folgenden Geräte verwenden Enterprise-Konnektivität:

- BlackBerry 10
- iOS-Geräte mit Secure Work Space
- Android-Geräte mit Secure Work Space

Enterprise-Konnektivitäts-Profile dienen überdies zum Aktivieren von BlackBerry Secure Connect Plus für BlackBerry 10- KNOX Workspace- und Android for Work-Geräte. Weitere Informationen zu BlackBerry Secure Connect Plus finden Sie unter „Verwenden von BlackBerry Secure Connect Plus für sichere Verbindungen mit geschäftlichen Ressourcen“.

Bevor Sie beginnen: Erstellen Sie bei Bedarf ein Proxyprofil.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf + neben **Enterprise-Konnektivität**.

3. Geben Sie einen Namen und eine Beschreibung für das Profil ein. Jedes Enterprise-Konnektivitäts-Profil muss über einen eindeutigen Namen verfügen.
4. Führen Sie folgende Aktionen aus:
   a. Klicken Sie auf die Registerkarte eines Gerätetyps.
   b. Wenn Sie nicht möchten, dass ein iOS- oder ein Android-Gerät mit Enterprise-Konnektivität arbeitet, deaktivieren Sie die Enterprise-Konnektivität für das Gerät.
   c. Wenn Enterprise-Konnektivität aktiviert ist und Sie einen Proxy verwenden, wählen Sie ein Proxyprofil.
   d. Wenn Sie BlackBerry Secure Connect Plus für BlackBerry 10-, KNOX Workspace- oder Android for Work-Geräte aktivieren möchten, stellen Sie sicher, dass das Kontrollkästchen **BlackBerry Secure Connect Plus aktivieren** ausgewählt ist.
5. Wiederholen Sie Schritt 4 für jeden Gerätetyp in Ihrer Organisation.
6. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Weisen Sie Profilen einen Rang zu.

Verwandte Informationen

Verwenden von BlackBerry Secure Connect Plus für sichere Verbindungen mit geschäftlichen Ressourcen, auf Seite 107

Einrichten einer Authentifizierung bei einmaliger Anmeldung für Geräte

Mithilfe einer einmaligen Anmeldung können Sie es BlackBerry 10-Geräten und bestimmten iOS-Geräten ermöglichen, sich bei Domänen und Webdiensten Ihres Unternehmensnetzwerks automatisch zu authentifizieren. Nach Zuweisung einer einmaligen Anmeldung wird der Benutzer aufgefordert, beim erstmaligen Zugriff auf eine von Ihnen festgelegte sichere Domäne einen Benutzernamen und ein Kennwort einzugeben. Die Anmeldeinformationen werden auf dem Gerät des Benutzers gespeichert und automatisch verwendet, wenn er versucht, auf die in seinem Profil festgelegten sicheren Domänen zuzugreifen. Wenn der Benutzer das Kennwort ändert, wird er beim nächsten Zugriff auf eine sichere Domäne zur Eingabe aufgefordert.

Sie können auch mithilfe eines Profils für die einmalige Anmeldung vertrauenswürdige Domänen für Zertifikate angeben, die Sie mit einem SCEP-Profil an BlackBerry 10-Geräte senden. Wenn Sie vertrauenswürdige Domänen festlegen, können BlackBerry 10-Benutzer die erforderlichen Zertifikate beim Zugriff auf eine vertrauenswürdige Domäne auswählen.

Profile für die einmalige Anwendung unterstützen die folgenden Authentifizierungstypen:

Authentifizierungstyp	Geräte-OS	Gilt für
• Kerberos	iOS	• Browser und Apps • Kann einschränken, von welchen Apps das Profil verwendet werden kann
	BlackBerry 10 OS	• Browser und Apps im geschäftlichen Bereich

Authentifizierungstyp	Geräte-OS	Gilt für
• NTLM • Festlegen vertrauenswürdiger Domänen für SCEP-Zertifikate	BlackBerry 10 OS	• Browser und Apps im geschäftlichen Bereich

Voraussetzungen: Verwenden der Kerberos-Authentifizierung für BlackBerry 10-Geräte

Zur Konfiguration der Kerberos-Authentifizierung für bestimmte Domänen können Sie die Kerberos-Konfigurationsdatei Ihrer Organisation (krb5.conf) hochladen. BES12 unterstützt die Heimdal-Implementierung von Kerberos.

Stellen Sie sicher, dass die Konfigurationsdatei die folgenden Anforderungen erfüllt:

- Die Kerberos-Konfiguration muss standardmäßig TCP anstelle von UDP verwenden. Verwenden Sie das Präfix tcp/ für KDC-Hosts.
- Wenn Ihre Organisation VPN verwendet, muss der VPN-Gateway Verkehr zu den KDCs zulassen.

Zertifikatbasierte Authentifizierung für iOS Version 8 und höher

Bei Geräten, auf denen iOS Version 8.0 und höher ausgeführt wird, können Sie Zertifikate zum Authentifizieren von iOS-Geräten mit Domänen und Webdiensten in Ihrem Unternehmensnetzwerk verwenden. Sie können einem Profil zur einmaligen Anmeldung ein freigegebenes Zertifikatprofil, ein SCEP-Profil oder ein Profil für Benutzeranmeldeinformationen hinzufügen. Wenn der Browser oder die Apps auf iOS-Geräten die zertifikatbasierte einmalige Anmeldung verwenden, werden die Benutzer automatisch authentifiziert (solange das Zertifikat gültig ist). Sie müssen keine Anmeldeinformationen eingeben, wenn sie auf die von Ihnen festgelegten sicheren Domänen zugreifen.

Erstellen eines Profils für die einmalige Anmeldung

Bevor Sie beginnen:

- Wenn Sie die Kerberos-Authentifizierung für BlackBerry 10-Geräte konfigurieren möchten, suchen Sie die Kerberos-Konfigurationsdatei Ihrer Organisation (krb5.conf).
- Wenn Sie die zertifikatbasierte Authentifizierung für Geräte verwenden möchten, auf denen iOS Version 8.0 und höher ausgeführt wird, erstellen Sie das erforderliche Profil für ein freigegebenes Zertifikat oder das SCEP-Profil.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf + neben **Einmalige Anmeldung**.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
4. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Konfigurieren der Kerberos-Authentifizierung für iOS-Geräte	1. Klicken Sie auf die Registerkarte **iOS**. 2. Klicken Sie unter **Kerberos** auf +. 3. Geben Sie im Feld **Name** einen Namen für die Konfiguration ein. 4. Geben Sie im Feld **Prinzipalname** den Namen des Kerberos-Prinzipals im Format <*primary*>/<*instance*>@<*realm*> (z. B. **user/admin@blackberry.example.com**) ein. 5. Geben Sie im Feld **Bereich** den Kerberos-Bereich in Großbuchstaben (z. B. **EXAMPLE.COM**) ein. 6. Geben Sie im Feld **URL-Präfixe** das URL-Präfix für die Websites ein, mit dem sich Geräte authentifizieren sollen. Das Präfix muss mit http:// oder https:// beginnen und kann Platzhalterwerte (*) enthalten (z. B. **https://www.blackberry.example.com/***). 7. Um mehr URL-Präfixe festzulegen, klicken Sie auf +, um weitere Felder hinzuzufügen. 8. Wenn Sie die Konfiguration auf bestimmte Apps einschränken möchten, klicken Sie auf + neben **App-Bezeichner**. Geben Sie die App-Bundle-ID ein. Sie können einen Platzhalterwert (*) verwenden, um die ID mit mehreren Apps abzugleichen. (z. B. **com.company.***). 9. Um mehr App-Bezeichner festzulegen, klicken Sie auf +, um weitere Felder hinzuzufügen. 10. Wenn Geräte, auf denen iOS Version 8.0 und höher ausgeführt wird, die zertifikatbasierte Authentifizierung verwenden sollen, klicken Sie in der Dropdown-Liste **Anmeldeinformationen** auf **Zertifikat**, **SCEP** oder **Benutzeranmeldeinformationen**. Klicken Sie in der Dropdown-Liste „Zertifikat“ auf das Zertifikatprofil, das Sie verwenden möchten. 11. Klicken Sie auf **Hinzufügen**. 12. Wiederholen Sie ggf. die Schritte 2 bis 11, um eine weitere Kerberos-Konfiguration hinzuzufügen.
Konfigurieren der Kerberos-Authentifizierung für BlackBerry 10-Geräte	1. Klicken Sie auf die Registerkarte **BlackBerry**. 2. Klicken Sie auf **Durchsuchen**. Navigieren Sie zur Kerberos-Konfigurationsdatei Ihrer Organisation (krb5.conf), und wählen Sie diese aus.
Konfigurieren der NTLM-Authentifizierung oder vertrauenswürdiger Domänen für	1. Klicken Sie auf die Registerkarte **BlackBerry**. 2. Klicken Sie unter **Vertrauenswürdige Domänen** auf +.

Aufgabe	Schritte
SCEP-Zertifikate für BlackBerry 10-Geräte	3. Geben Sie im Feld **Name** einen Namen für die Konfiguration ein. 4. Geben Sie im Feld **Domäne** eine vertrauenswürdige Unterdomäne oder einen einzelnen Host ein, auf dem die Anmeldeinformationen für die Domäne zur automatischen Authentifizierung verwendet werden können. Geben Sie den Servernamen als einen FQDN, Hostnamen, Alias-Namen oder eine IP-Adresse ein. DNS-Namen können Platzhalter (*) enthalten. 5. Um mehr Unterdomänen festzulegen, klicken Sie auf +, um weitere Felder hinzuzufügen. 6. Klicken Sie auf **Hinzufügen**. 7. Wiederholen Sie ggf. die Schritte 2 bis 6, um eine weitere vertrauenswürdige Domäne hinzuzufügen.

5. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Wenn Sie mehr als ein Profil für die einmalige Anmeldung erstellen, weisen Sie den Profilen einen Rang zu.

Verwandte Informationen

Erstellen von Profilen für freigegebene Zertifikate, auf Seite 74
Erstellen von SCEP-Profilen, auf Seite 73

Verwenden von BlackBerry Secure Connect Plus für sichere Verbindungen mit geschäftlichen Ressourcen

16

Die BES12-Komponente BlackBerry Secure Connect Plus bietet einen sicheren IP-Tunnel zwischen Apps für den geschäftlichen Bereich auf BlackBerry 10-, Samsung KNOX Workspace- und Android for Work-Geräten und dem Netzwerk des Unternehmens. Über diesen Tunnel haben Benutzer Zugriff auf Ressourcen hinter der Firewall des Unternehmens, wobei die Sicherheit der Daten mithilfe von Standardprotokollen und durchgehender Verschlüsselung sichergestellt wird.

BlackBerry Secure Connect Plus und unterstützte Geräte erstellen einen sicheren IP-Tunnel, wenn dies die beste Wahl für eine Verbindung mit dem Netzwerk des Unternehmens ist. Ist einem Gerät ein Wi-Fi oder VPN-Profil zugewiesen, und das Gerät hat Zugriff auf das geschäftliche Wi-Fi- bzw. VPN-Netzwerk, wird diese Methode zum Herstellen einer Verbindung verwendet. Stehen diese Möglichkeiten nicht zur Verfügung (z. B. wenn der Benutzer sich außerhalb des geschäftlichen Wi-Fi-Funkbereichs befindet), stellen BlackBerry Secure Connect Plus und das Gerät einen sicheren IP-Tunnel her.

Unterstützte Geräte kommunizieren zur Herstellung des sicheren Tunnels über die BlackBerry Infrastructure mit BES12. Für jedes Gerät wird ein Tunnel erstellt. Der Tunnel unterstützt Standard-IPv4-Protokolle (TCP und UDP). Solange der Tunnel geöffnet ist, hat jede App im geschäftlichen Bereich Zugriff auf Netzwerkressourcen. Sobald der Tunnel nicht mehr benötigt wird (zum Beispiel, wenn der Benutzer in den Empfangsbereich des geschäftlichen Wi-Fi-Netzwerks zurückkehrt), wird er geschlossen.

BlackBerry Secure Connect Plus bietet die folgenden Vorteile:

- IP-Datenverkehr zwischen Geräten und BES12 wird komplett verschlüsselt, wodurch die Sicherheit geschäftlicher Daten gewährleistet wird.
- BlackBerry Secure Connect Plus bietet eine sichere, zuverlässige Verbindung mit geschäftlichen Ressourcen, wenn ein Benutzer nicht auf das geschäftliche Wi-Fi-Netzwerk oder VPN zugreifen kann.
- BlackBerry Secure Connect Plus wird hinter der Firewall des Unternehmens installiert, sodass Daten in einem vertrauenswürdigen Bereich übertragen werden, der die Sicherheitsstandards des Unternehmens erfüllt.

Schritte zum Aktivieren von BlackBerry Secure Connect Plus

Beim Aktivieren von BlackBerry Secure Connect Plus führen Sie die folgenden Aktionen aus:

Schritt	Aktion
1	Sicherstellen, dass die BES12-Domäne im Unternehmen die Anforderungen zur Verwendung von BlackBerry Secure Connect Plus erfüllt

Schritt	Aktion
2	Sicherstellen, dass BlackBerry Secure Connect Plus im Standard-Enterprise-Konnektivitäts-Profil oder in einem von Ihnen erstellten benutzerdefinierten Enterprise-Konnektivitäts-Profil aktiviert ist
3	Optional: Festlegen der DNS-Einstellungen für die BES12 Secure Connect Plus-App
4	Zuweisen des Enterprise-Konnektivitäts-Profils zu Benutzern

Verwandte Informationen

Aktivieren von BlackBerry Secure Connect Plus, auf Seite 110
Festlegen der DNS-Einstellungen für die BES12 Secure Connect Plus-App, auf Seite 111
Zuweisen eines Profils zu einer Benutzergruppe, auf Seite 204
Zuweisen eines Profils zu einem Benutzerkonto, auf Seite 219
Anforderungen an Server und Geräte, auf Seite 108

Anforderungen an Server und Geräte

Zur Verwendung von BlackBerry Secure Connect Plus muss die Umgebung des Unternehmens folgende Anforderungen erfüllen.

BES12-Domäne:

- Die Firewall muss ausgehende Verbindungen über Port 3101 mit *<region>*.turnb.bbsecure.com und *<region>*.bbsecure.com zulassen. Wenn Sie BES12 zur Verwendung eines Proxyservers konfigurieren, muss dieser Verbindungen über Port 3101 mit diesen Unterdomänen zulassen. Weitere Informationen zu den Domänen und IP-Adressen für die Firewall-Konfiguration finden Sie in Artikel KB36470 unter www.blackberry.com/go/kbhelp.
- In jeder BES12-Instanz muss die BlackBerry Secure Connect Plus-Komponente ausgeführt werden.

Unterstützte Geräte:

Gerät	Anforderungen
BlackBerry 10	• BlackBerry 10 OS Version 10.3.2 oder höher • Eine der folgenden Aktivierungsarten: ◦ Geschäftlich und persönlich – Unternehmen ◦ Nur geschäftlicher Bereich ◦ Geschäftlich und persönlich – Reguliert
Samsung KNOX Workspace	• Android OS Version 5.0 oder höher

Gerät	Anforderungen
	• Samsung KNOX MDM Version 5.0 oder höher • Samsung KNOX 2.1 oder höher • Eine der folgenden Aktivierungsarten: ◦ Nur geschäftlicher Bereich - Samsung KNOX ◦ Geschäftlich und persönlich – vollständige Kontrolle - Samsung KNOX
Android for Work	• Android OS 5.1 oder höher • Aktivierungsart „ Geschäftlich und persönlich – Benutzer-Datenschutz (Android for Work - Premium)“

Weitere Informationen zu den für die einzelnen Aktivierungsarten erforderlichen Lizenzen finden Sie in der Dokumentation zur Lizenzierung unter help.blackberry.com/detectLang/bes12/.

Datenfluss bei der Erstellung eines sicheren IP-Tunnels durch BlackBerry Secure Connect Plus

1. BES12 und Gerät erkennen, dass ein sicherer IP-Tunnel die beste verfügbare Methode zur Verbindung zwischen Apps im geschäftlichen Bereich und dem Netzwerk des Unternehmens ist.
2. Das Gerät sendet ein Signal über einen TLS-Tunnel und Port 443 an die BlackBerry Infrastructure, um einen sicheren Tunnel zum Netzwerk des Unternehmens anzufordern. Das Signal wird standardmäßig unter Verwendung FIPS-140-zertifizierter Certicom-Bibliotheken mit Cipher Suites für RSA und ECC-Schlüsseln verschlüsselt. Der Tunnel für das Signal ist komplett verschlüsselt.
3. BlackBerry Secure Connect Plus empfängt das Signal über Port 3101 von der BlackBerry Infrastructure.
4. Das Gerät und BlackBerry Secure Connect Plus handeln die Tunnelparameter aus und erstellen einen sicheren Tunnel über TURN durch die BlackBerry Infrastructure. Der Tunnel ist authentifiziert und durchgehend mit DTLS verschlüsselt.
    - Für jedes Gerät wird ein Tunnel erstellt. Alle Apps im geschäftlichen Bereich können über den Tunnel eine Verbindung mit den geschäftlichen Ressourcen erstellen.
5. BlackBerry Secure Connect Plus überträgt IP-Datenverkehr (Datenpakete) an die und von den Netzwerkressourcen.
    - Der Tunnel unterstützt Standard-IPv4-Protokolle (TCP und UDP).
    - BlackBerry Secure Connect Plus verschlüsselt und entschlüsselt Datenverkehr mit FIPS-140-zertifizierten Certicom-Bibliotheken mit Cipher Suites für RSA und ECC-Schlüsselnaktiviert werden.

6. BlackBerry Secure Connect Plus schließt den Tunnel, sobald dieser nicht mehr die beste Methode der Verbindung von Apps im geschäftlichen Bereich mit Netzwerkressourcen ist.

BlackBerry Secure Connect Plus kann mehrere Tunnel über eine einzelne TURN-Zuordnung in der BlackBerry Infrastructure erstellen. Jeder Tunnel wird für ein anderes Gerät verwendet und besitzt eine eindeutige ID sowie einen eindeutigen DTLS-Kontext.

Lastverteilung und hohe Verfügbarkeit für BlackBerry Secure Connect Plus

Wenn es in einer Domäne mehrere BES12-Instanzen gibt, wird die BlackBerry Secure Connect Plus-Komponente in jeder Instanz ausgeführt und verarbeitet Daten. Für die Daten erfolgt eine Lastverteilung über alle BlackBerry Secure Connect Plus-Komponenten in der Domäne.

Failover für hohe Verfügbarkeit ist für BlackBerry 10-, Samsung KNOX Workspace- und Android for Work-Geräte verfügbar. Wenn ein Gerät einen sicheren Tunnel verwendet und die aktuelle BlackBerry Secure Connect Plus-Komponente unverfügbar wird, weist die BlackBerry Infrastructure das Gerät einer BlackBerry Secure Connect Plus-Komponente einer anderen BES12-Instanz zu. Das Gerät nimmt die Verwendung des sicheren Tunnels mit minimaler Unterbrechung wieder auf.

Aktivieren und Konfigurieren von BlackBerry Secure Connect Plus

Führen Sie die Aufgaben in diesem Abschnitt durch, um BlackBerry Secure Connect Plus für Gerätebenutzer zu aktivieren und zu konfigurieren.

Sie aktivieren BlackBerry Secure Connect Plus unter Verwendung eines Enterprise-Konnektivitäts-Profils. Im Fall von BlackBerry 10Geräten ist BlackBerry Secure Connect Plus mit Enterprise-Konnektivitäts-Profilen verknüpft. Sie können die Enterprise-Konnektivität für BlackBerry 10-Geräte nicht deaktivieren. Im Fall von Android-Geräten gilt die Enterprise-Konnektivität spezifisch für Geräte mit Secure Work Space, und BlackBerry Secure Connect Plus spezifisch für Samsung KNOX Workspace- und Android for Work-Geräte.

Aktivieren von BlackBerry Secure Connect Plus

Wenn Sie zulassen möchten, dass Geräte BlackBerry Secure Connect Plus verwenden, müssen Sie den Benutzern ein Enterprise-Konnektivitäts-Profil zuweisen, in dem BlackBerry Secure Connect Plus aktiviert ist. BlackBerry Secure Connect Plus ist standardmäßig für BlackBerry 10- und unterstützte Android-Geräte aktiviert. Folgende Optionen sind möglich:

- Vergewissern Sie sich, dass BlackBerry Secure Connect Plus im standardmäßigen Enterprise-Konnektivitäts-Profil aktiviert ist. Wird einem Benutzerkonto kein benutzerdefiniertes Enterprise-Konnektivitäts-Profil direkt oder per Gruppenmitgliedschaft zugewiesen, weist BES12 das Standardprofil zu.

- Erstellen Sie ein benutzerdefiniertes Enterprise-Konnektivitäts-Profil anhand der nachfolgenden Anweisungen, und weisen Sie es den Benutzern oder Gruppen zu.

Wenn das Enterprise-Konnektivitäts-Profil auf ein Gerät nach dessen Aktivierung angewendet wird, sendet BES12 das zur Verwendung von BlackBerry Secure Connect Plus erforderliche SCEP- und VPN-Profil an das Gerät. BES12 installiert außerdem die BES12 Secure Connect Plus-App auf dem Gerät (auf Android for Work-Geräten wird die App automatisch aus Google Play installiert). Auf BlackBerry 10-Geräten ist die App verborgen und erfordert keine Benutzerinteraktion.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien und Profile**.
2. Klicken Sie im linken Fensterbereich auf + neben **Enterprise-Konnektivität**.
3. Führen Sie eine der folgenden Aktionen aus:
   - Vergewissern Sie sich, dass auf der Registerkarte **BlackBerry** das Kontrollkästchen **BlackBerry Secure Connect Plus aktivieren** ausgewählt ist.
   - Vergewissern Sie sich, dass auf der Registerkarte **Android** das Kontrollkästchen **BlackBerry Secure Connect Plus aktivieren** ausgewählt ist.
4. Wenn Sie Enterprise-Konnektivitäts-Datenverkehr von BlackBerry 10-Geräten an BlackBerry Secure Connect Plus durch einen dem Unternehmensnetzwerk vorgeschalteten Proxyserver routen möchten, wählen Sie auf der Registerkarte **BlackBerry** in der Dropdown-Liste **Proxyprofil** das entsprechende Proxyprofil aus.

   Die Proxyprofileinstellung auf der Registerkarte **Android** gilt nur für Enterprise-Konnektivität bei Geräten, auf denen Secure Work Space verwendet wird, nicht aber bei solchen, auf denen BlackBerry Secure Connect Plus verwendet wird.
5. Klicken Sie auf **Hinzufügen**.
6. Weisen Sie das Profil Benutzergruppen bzw. Benutzerkonten zu.

Wenn Sie fertig sind:

- Wenn Sie mehrere Enterprise-Konnektivitäts-Profile erstellt haben, weisen Sie ihnen eine Rangordnung zu.
- Auf Samsung KNOX Workspace- und Android for Work-Geräten werden Benutzer von der BES12 Secure Connect Plus-App aufgefordert, die Ausführung als VPN und den Zugriff auf private Schlüssel auf dem Gerät zuzulassen. Weisen Sie die Benutzer an, dieser Aufforderung nachzukommen. Die Benutzer können die App zum Anzeigen des Status der Verbindung öffnen. Zur Verwendung von BlackBerry Secure Connect Plus sind keine weiteren Maßnahmen von den Benutzern erforderlich.

Festlegen der DNS-Einstellungen für die BES12 Secure Connect Plus-App

Sie können den DNS-Server festlegen, der von der BES12 Secure Connect Plus-App auf BlackBerry 10-, Samsung KNOX Workspace- und Android for Work-Geräten für sichere Tunnel-Verbindungen verwendet werden soll. Sie können außerdem Suffixe für die DNS-Suche angeben. Wenn Sie keine DNS-Einstellungen festlegen, bezieht die App DNS-Adressen von dem Computer, der die BlackBerry Secure Connect Plus-Komponente hostet, und als standardmäßigen Suchsuffix wird die DNS-Domäne dieses Computers verwendet.

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Klicken Sie im linken Fensterbereich auf **Infrastruktur** > **BlackBerry Secure Connect Plus**.
3. Aktivieren Sie das Kontrollkästchen **DNS-Server manuell konfigurieren**, und klicken Sie auf +.
4. Geben Sie die Adresse des DNS-Servers in Dezimalschreibweise mit Punkt ein (zum Beispiel: 192.0.2.0). Klicken Sie auf **Hinzufügen**.
5. Wiederholen Sie ggf. die Schritte 3 und 4, um eine weitere DNS-Server hinzuzufügen. Klicken Sie in der Tabelle **DNS-Server** auf die Pfeile in der Spalte **Rangordnung**, um die Rangordnung der DNS-Server festzulegen.
6. Wenn Sie Suffixe für die DNS-Suche festlegen möchten, führen Sie die folgenden Schritte aus:
   a. Aktivieren Sie das Kontrollkästchen **DNS-Suchsuffixe manuell verwalten**, und klicken Sie auf +.
   b. Geben Sie die das DNS-Suchsuffix ein (z. B. domain.com). Klicken Sie auf **Hinzufügen**.
7. Wiederholen Sie ggf. Schritt 6, um eine weitere DNS-Suchsuffixe hinzuzufügen. Klicken Sie in der Tabelle **DNS-Suchsuffix** auf die Pfeile in der Spalte **Rangordnung**, um die Rangordnung der DNS-Server festzulegen.
8. Klicken Sie auf **Speichern**.

Leiten des geschäftlichen Datenverkehrs in BlackBerry 10 über BlackBerry Secure Connect Plus, wenn einWi-Fi-Netzwerk verfügbar ist

Wenn Sie mit BES12 ein Wi-Fi-Profil konfigurieren und BlackBerry 10-Geräten zuweisen, wird auf den Geräten dem geschäftlichen Wi-Fi-Netzwerk Vorrang vor BlackBerry Secure Connect Plus gegeben. Steht das geschäftliche Wi-Fi-Netzwerk nicht zur Verfügung, und den Geräten ist kein VPN-Profil zugewiesen oder sie haben keinen VPN-Zugriff, wird BlackBerry Secure Connect Plus verwendet. Sie können den gesamten geschäftlichen Datenverkehr über BlackBerry Secure Connect Plus leiten, selbst wenn Geräte Zugriff auf das Wi-Fi-Netzwerk haben. Diese Option kann beispielsweise dann verwendet werden, wenn die Sicherheitsstandards im Unternehmen Geräteverbindungen mit geschäftlichen Ressourcen über das Wi-Fi-Netzwerk nicht zulassen.

Hinweis: Durch die Aktivierung dieser Funktion wird der gesamte geschäftliche Datenverkehr, für den normalerweise das Wi-Fi-Netzwerk verwendet würde, über eine sichere Verbindung mit der BlackBerry Infrastructure geleitet. Diese Funktion kann Auswirkungen auf Datennutzungs- und Netzwerkkosten Ihres Unternehmens haben. Vergewissern Sie sich, dass dies die bevorzugte Konfiguration im Unternehmen ist, bevor Sie diese Funktion aktivieren.

Bevor Sie beginnen: Vergewissern Sie sich, dass in der den Benutzern von BlackBerry 10-Geräten zugewiesenen IT-Richtlinie die IT-Richtlinienregel „Steuerung des Netzwerkzugriffs für geschäftliche Apps erzwingen“ nicht ausgewählt ist.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Erweitern Sie im linken Fensterbereich **Wi-Fi**, und klicken Sie auf das Wi-Fi-Profil, das Benutzern von BlackBerry 10-Geräten zugewiesen ist.
3. Klicken Sie auf ✎.

4. Aktivieren Sie auf der Registerkarte **BlackBerry** im Bereich **Verknüpfte Profile** das Kontrollkästchen **Enterprise-Konnektivitäts-Profil mit BlackBerry Secure Connect Plus-Verbindung für geschäftliche Daten verwenden**.
5. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Wenn Sie mehrere Wi-Fi-Profile erstellt und zugewiesen, wiederholen Sie diese Schritte entsprechend.

Verwandte Informationen
BlackBerry 10: Wi-Fi-Profileinstellungen, auf Seite 369

Fehlerbehebung bei BlackBerry Secure Connect Plus

BlackBerry Secure Connect Plus-Adapter wechselt in den Zustand „Nicht identifizierter Netzwerk“ und funktioniert nicht mehr

Ursache

Dieses Problem kann auftreten, wenn Sie den Computer, auf dem BES12 gehostet wird, neu starten.

Lösung für Windows Server 2008 R2 und Windows Server 2008 R2 SP1

1. Erweitern Sie im Server-Manager **Rollen** > **Netzwerkrichtlinien- und Zugriffsdienste**. Klicken Sie mit der rechten Maustaste auf **Routing und Remotezugriff** und dann auf **Routing und RAS deaktivieren**.
2. Klicken Sie mit der rechten Maustaste auf **Routing und Remotezugriff** und dann auf **Routing und RAS konfigurieren und aktivieren**.
3. Schließen Sie den Setup-Assistenten unter Auswahl folgender Optionen ab:
   a. Wählen Sie im Bildschirm **Konfiguration** die Option **Netzwerkadressenübersetzung (NAT)**.
   b. Wählen Sie im Bildschirm **NAT-Internetverbindung** die Option **Diese öffentliche Schnittstelle zum Herstellen der Internetverbindung verwenden** . Vergewissern Sie sich, dass BlackBerry Secure Connect Plus in der Liste der Netzwerkschnittstellen angezeigt wird.
4. Erweitern Sie **Rollen** > **Netzwerkrichtlinien- und Zugriffsdienste** > **Routing und Remotezugriff** > **IPv4**, und klicken Sie auf **NAT**. Öffnen Sie die Eigenschaften von **LAN-Verbindung**, und wählen Sie **An das Internet angeschlossene, öffentliche Schnittstelle** und **NAT auf dieser Schnittstelle aktivieren**. Klicken Sie auf **OK**.
5. Öffnen Sie die Eigenschaften von **BlackBerry Secure Connect Plus**, und wählen Sie **An ein privates Netzwerk angeschlossene, private Schnittstelle**. Klicken Sie auf **OK**.
6. Klicken Sie mit der rechten Maustaste auf **Routing und Remotezugriff** und dann auf **Alle Tasks** > **Neu starten**.
7. Starten Sie in den Windows-Diensten den Dienst **BES12 – BlackBerry Secure Connect Plus**.

Es kann ein paar Minuten dauern bis der BlackBerry Secure Connect Plus-Adapter unter „Netzwerkverbindungen“ eine erfolgreiche Verbindung anzeigt.

Laden und installieren Sie den Hotfix im Windows-KB-Artikel NAT functionality fails on a Windows Server 2008 R2 SP1-based RRAS server.

Lösung für Windows Server 2012

1. Klicken Sie im Server-Manager auf **Verwalten** > **Rollen und Features hinzufügen**. Klicken Sie so oft auf **Weiter**, bis der Bildschirm **Features** angezeigt wird. Erweitern Sie **Remoteserver-Verwaltungstools** > **Rollenverwaltungstools**, und wählen Sie **Tools für die Remotezugriffsverwaltung**. Schließen Sie den Assistenten zum Installieren der Tools ab.
2. Klicken Sie auf **Extras** > **Remotezugriffsverwaltung**.
3. Klicken Sie unter **Konfiguration** auf **DirectAccess und VPN**.
4. Klicken Sie unter **VPN** auf **RRAS-Verwaltung öffnen**.
5. Klicken Sie mit der rechten Maustaste auf den Routing- und RAS-Server und dann auf **Routing und RAS deaktivieren**.
6. Klicken Sie mit der rechten Maustaste auf den Routing- und RAS-Server und dann auf **Routing und RAS konfigurieren und aktivieren**.
7. Schließen Sie den Setup-Assistenten unter Auswahl folgender Optionen ab:
   a. Wählen Sie im Bildschirm **Konfiguration** die Option **Netzwerkadressenübersetzung (NAT)**.
   b. Wählen Sie im Bildschirm **NAT-Internetverbindung** die Option **Diese öffentliche Schnittstelle zum Herstellen der Internetverbindung verwenden** . Vergewissern Sie sich, dass BlackBerry Secure Connect Plus in der Liste der Netzwerkschnittstellen angezeigt wird.
8. Erweitern Sie **Rollen** > **Netzwerkrichtlinien- und Zugriffsdienste** > **Routing und Remotezugriff** > **IPv4**, und klicken Sie auf **NAT**. Öffnen Sie die Eigenschaften von **LAN-Verbindung**, und wählen Sie **An das Internet angeschlossene, öffentliche Schnittstelle** und **NAT auf dieser Schnittstelle aktivieren**. Klicken Sie auf **OK**.
9. Öffnen Sie die Eigenschaften von **BlackBerry Secure Connect Plus**, und wählen Sie **An ein privates Netzwerk angeschlossene, private Schnittstelle**. Klicken Sie auf **OK**.
10. Klicken Sie mit der rechten Maustaste auf den Routing- und RAS-Server und dann auf **Alle Tasks** > **Neu starten**.
11. Starten Sie in den Windows-Diensten den Dienst **BES12 – BlackBerry Secure Connect Plus**.

Anzeigen der Protokolldateien für BlackBerry Secure Connect Plus

Daten über BlackBerry Secure Connect Plus werden in zwei Protokolldateien aufgezeichnet:

- BSCP: Protokolldaten zur BlackBerry Secure Connect Plus-Serverkomponente
- BSCP-TS: Protokolldateien zu Verbindungen mit der BES12 Secure Connect Plus-App

Beide Protokolldateien befinden sich im Ordner <*drive*>:\Programme\BlackBerry\BES\Logs\<*yyyymmdd*>.

Zweck	Protokoll-datei	Beispiel
Prüfen, ob BlackBerry Secure Connect Plus mit der BlackBerry Infrastructure verbunden ist	BSCP	2015-01-19T13:17:47.540-0500 - BSCP {TcpClientConnectorNio#2} logging.feature.bscp.service|logging.component.bscp.pss.bcp [{}] - DEBUG Received Ping from [id: 0x60bce5a3, /10.90.84.22:28231 => stratos.bcp.bblabs.rim.net/206.53.155.152:3101], responding with Pong. 2015-01-19T13:18:22.989-0500 - BSCP {ChannelPinger#1} logging.feature.bscp.service|logging.component.bscp.pss.bcp [{}] - DEBUG Sending Ping to [id: 0xb4a1677a, /10.90.84.22:28232 => stratos.bcp.bblabs.rim.net/206.53.155.152:3101]
Prüfen, ob BlackBerry Secure Connect Plus Aufrufe aus der BES12 Secure Connect Plus-App auf Geräten empfangen kann	BSCP-TS	47: [14:13:21.231312][][3][AsioTurnSocket-1] Connected, host=68-171-243-141.rdns.blackberry.net 48: [14:13:21.239312][][3][AsioTurnSocket-1] Creating TURN allocation 49: [14:13:21.405121][][3][AsioTurnSocket-1] TURN allocation created
Prüfen, ob Geräte den sicheren Tunnel verwenden	BSCP-TS	74: [10:39:45.746926][][3][Tunnel-2FFEC51E] Sent: 2130.6 KB (1733), Received: 201.9 KB (1370), Running: 00:07:00.139249

Verwandte Informationen

Verwendung von Protokolldateien, auf Seite 282

Gerätestandards

Definieren und erzwingen Sie Organisationsstandards und andere Bedingungen auf Geräten.

Simple

Einrichten der Gerätestandards für Ihre Organisation

17

Sie können Profile verwenden, um bestimmte Standards für die Geräte in Ihrer Organisation durchzusetzen. Verschiedene Profile unterstützen bestimmte Konfigurationen wie Kompatibilitätsregeln, Einschränkungen bei Webinhalte oder App-Einschränkungen. Sie können Einstellungen für BlackBerry 10-, iOS-, Android- und Windows Phone-Geräte in dem gleichen Profil festlegen und das Profil dann Benutzerkonten, Benutzergruppen oder Gerätegruppen zuweisen.

Schritte zum Einrichten der Gerätestandards für Ihre Organisation

Führen Sie zum Einrichten der Gerätestandards für Ihre Organisation die folgenden Aktionen aus:

Schritt	Aktion
1	Erstellen Sie Profile, um bestimmte Standards auf Geräten voreinzustellen.
2	Legen Sie ggf. eine Rangfolge für die Profile fest.
3	Weisen Sie Benutzerkonten, Benutzergruppen oder Gerätegruppen Profile zu.

Verwalten der Standards Ihrer Organisation mit Profilen

Sie können bestimmte Standards für Geräte über die in der Bibliothek „Richtlinien und Profile“ verfügbaren Profile verwalten.

Profil	Beschreibung
Kompatibilität	Ein Kompatibilitätsprofil definiert die Gerätebedingungen, die in Ihrer Organisation nicht akzeptabel sind, und legt entsprechende Durchsetzungsaktionen fest. BES12 enthält ein Standard-Kompatibilitätsprofil.

Profil	Beschreibung
Webinhaltsfilter	Ein Webinhaltsfilter-Profil schränkt die Websites ein, die ein Benutzer auf überwachten iOS-Geräten aufrufen kann.
App-Sperrmodus	Ein App-Sperrmodus-Profil konfiguriert überwachte iOS-Geräte und Geräte, die mit KNOX MDM verwaltet werden, sodass sie nur eine App ausführen (beispielsweise zu Schulungszwecken oder für Point-of-Sales-Demonstrationen).
Gerätedienstanforderungen	Ein Profil für Gerätedienstanforderungen definiert die Softwareversionen, die auf BlackBerry 10-Geräten installiert sein müssen.
Verwaltete Domänen	Ein Profil für verwaltete Domänen konfiguriert Geräte mit iOS 8 so, dass Benutzer benachrichtigt werden, wenn sie E-Mails außerhalb von vertrauenswürdigen Domänen senden, und es schränkt die Apps ein, die aus internen Domänen heruntergeladene Dokumente anzeigen können.
Gerät	Ein Geräteprofil gestattet die Konfiguration der Informationen, die auf Geräten angezeigt werden.
Websymbol	Mit einem Websymbol-Profil können Sie ein benutzerdefiniertes Websymbol zur Anzeige auf iOS-Geräten erstellen.
Standortbestimmung	Ein Profil für die Standortbestimmung ermöglicht das Orten von iOS-Geräten auf einer Karte.

Durchsetzen von Kompatibilitätsregeln für Geräte

Sie können Kompatibilitätsprofile verwenden, um Gerätebenutzer bei der Einhaltung der in Ihrer Organisation in Bezug auf die Verwendung von BlackBerry 10-, iOS-, Android- und Windows Phone-Geräten festgelegten Standards zu unterstützen. Ein Kompatibilitätsprofil definiert die Gerätebedingungen, die in Ihrer Organisation nicht akzeptabel sind. Sie können beispielsweise festlegen, dass Geräte, die entsperrt oder gehackt sind oder für die aufgrund eines nicht autorisierten Zugriffs auf das Betriebssystem ein Integritätsalarm vorliegt, nicht zulässig sind.

Ein Kompatibilitätsprofil legt die folgenden Informationen fest:

- Bedingungen, aufgrund derer ein Gerät mit BES12 nicht kompatibel ist
- Benachrichtigungen, die die Benutzer erhalten, wenn sie die Kompatibilitätsbedingungen verletzen, und die Zeitdauer, die Benutzern zur Behebung des Problems zur Verfügung steht
- Benachrichtigungen, die die Benutzer erhalten, wenn sie gesperrte Apps installieren, und die Zeitdauer, die Benutzern zur Behebung des Problems zur Verfügung steht

- Eine Aktion, die vorgenommen wird, wenn der Benutzer das Problem nicht behebt, einschließlich der Einschränkung des Benutzerzugriffs auf die Ressourcen der Organisation, Löschen geschäftlicher Daten auf dem Gerät oder Löschen aller Daten auf dem Gerät

Bei Android-Geräten, die KNOX-MDM verwenden, können Sie eine Liste der gesperrten Apps zu einem Kompatibilitätsprofil hinzufügen. BES12 setzt jedoch nicht die Kompatibilitätsregeln durch. Stattdessen wird die Liste mit den gesperrten Apps an die Geräte gesendet, die daraufhin die Einhaltung erzwingen. Gesperrte Apps können nicht installiert werden, und wenn sie bereits installiert sind, werden sie deaktiviert. Wenn Sie eine App aus der Liste der gesperrten Apps entfernen, wird die App erneut aktiviert (sofern sie bereits installiert ist). Informationen dazu, welche Android-Geräte KNOX-MDM unterstützen, finden Sie in der Kompatibilitätsmatrix unter help.blackberry.com/detectLang/bes12/current/compatibility-matrix-pdf/.

BES12 enthält ein Standard-Kompatibilitätsprofil. Standardmäßig setzt das Standard-Kompatibilitätsprofil keine Kompatibilitätsbedingungen durch. Um Kompatibilitätsregeln durchzusetzen, können Sie die Einstellungen des Standard-Kompatibilitätsprofils ändern oder benutzerdefinierte Kompatibilitätsprofile erstellen und zuweisen. Benutzerkonten, denen kein benutzerdefiniertes Kompatibilitätsprofil zugewiesen wird, wird das Standard-Kompatibilitätsprofil zugewiesen.

Erstellen eines Kompatibilitätsprofils

Bevor Sie beginnen:

- Wenn Sie Regeln für gesperrte Apps definieren, fügen Sie die jeweiligen Apps der Liste der gesperrten Apps hinzu. Weitere Informationen finden Sie unter „Hinzufügen einer App zur Liste der gesperrten Apps“.
- Um Windows-Apps in Kompatibilitätsprofilen zu überwachen, müssen Sie einen AET hochladen. Weitere Informationen finden Sie unter „Hochladen eines Anwendungsinstallations-Tokens (AET)“.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf + neben **Kompatibilität**.
3. Geben Sie einen Namen und eine Beschreibung für das Kompatibilitätsprofil ein.
4. Klicken Sie auf die Registerkarte für den entsprechenden Gerätetyp, und führen Sie die folgenden Aktionen aus:
    - Wenn Geräte mit einer Betriebssystemverletzung als nicht konform gelten sollen, aktivieren Sie das Kontrollkästchen **Integritätsalarm** (BlackBerry 10), **Betriebssystem mit Jailbreak** (iOS) oder **Betriebssystem mit Root-Zugriff** (Android).
    - BlackBerry 10-Geräte: Wenn Geräte, die eine im Gerätedienstanforderungs-Profil aufgeführte gesperrte Software verwenden, als nicht konform gelten sollen, wählen Sie die Option **Eine gesperrte Softwareversion wurde installiert** aus. Diese Bedingung gilt nicht für Geräte mit der Aktivierungsart „Geschäftlich und persönlich – Unternehmen“.
    - Bei iOS- oder Android-Geräten: Wenn Geräte mit Apps, die Sie nicht installiert haben, als nicht konform gelten sollen, aktivieren Sie das Kontrollkästchen **Nicht zugewiesene App wurde installiert**. Diese Bedingung gilt nicht für Geräte mit der Aktivierungsart „Geschäftlich und persönlich – Benutzer-Datenschutz“.
    - Für iOS-, Android- und Windows Phone-Geräte:
        - Wenn Geräte, bei denen keine gesperrte App vorhanden ist, als nicht konform gelten sollen, aktivieren Sie das Kontrollkästchen **Eine erforderliche App ist nicht installiert**. Diese Bedingung gilt nicht für

Geräte mit der Aktivierungsart „Geschäftlich und persönlich – Benutzer-Datenschutz“. Bei Windows Phone-Geräten Version 8.0 können nur interne erforderliche Apps überwacht werden.

- Wenn Geräte, bei denen eine gesperrte App vorhanden ist, als nicht konform gelten sollen, aktivieren Sie das Kontrollkästchen **Eine gesperrte App wurde installiert**, und fügen Sie die gesperrten Apps der Tabelle hinzu. Diese Bedingung gilt nicht für Geräte mit der Aktivierungsart „Geschäftlich und persönlich – Benutzer-Datenschutz“.

5. Wählen Sie bei allen Geräten (ausgenommen Android-Geräte, die KNOX MDM verwenden) und für jede in Schritt 4 ausgewählte Bedingung die Aktion aus, die BES12 ausführen soll, wenn ein Benutzergerät als nicht konform eingestuft wird:

Aktion	Schritte
Automatische Benachrichtigung des Benutzers, dass sein Gerät nicht konform ist, und Durchführung einer Erzwingungsaktion, wenn der Benutzer das Problem nicht behebt.	1. Klicken Sie in der Dropdown-Liste **Erzwingungsaktion** auf **Vorschrifteneinhaltung fordern**. 2. Klicken Sie in der Dropdown-Liste **Aufforderungsmethode** auf den Nachrichtentyp, der an den Benutzer gesendet werden soll. 3. Geben Sie im Feld **Anzahl der Aufforderungen** ein, wie oft die Benachrichtigung gesendet werden soll, bevor BES12 die Aktion durchführt. 4. Legen Sie im Feld **Aufforderungsintervall** und in der Dropdown-Liste die Zeitdauer zwischen den Aufforderungen fest. 5. Klicken Sie in der Dropdown-Liste **Aktion bei Ablauf des Aufforderungsintervalls** auf die Aktion, die der BES12 bei Ablauf des Aufforderungsintervalls ausführen soll. • Wenn keine Erzwingungsaktion erfolgen soll, wählen Sie **Keine** aus. • Um zu verhindern, dass der Benutzer mit dem Gerät auf geschäftliche Ressourcen und Anwendungen zugreift, wählen Sie **Quarantäne** (BlackBerry 10) oder **Nicht vertrauen** (iOS oder Android) aus. Daten und Anwendungen werden nicht vom Gerät gelöscht. • Um Geschäftsdaten vom Gerät zu löschen, wählen Sie **Nur Geschäftsdaten löschen**. • Um alle Daten vom Gerät zu löschen, wählen Sie **Alle Daten löschen**. Auf Geräten, auf denen „Geschäftlich und persönlich – Unternehmen“ oder „Geschäftlich und persönlich – Benutzer-Datenschutz“ aktiviert ist, werden nur Geschäftsdaten gelöscht.

Aktion	Schritte
Verhindern Sie, dass der Benutzer auf geschäftliche Ressourcen und Anwendungen vom Gerät zugreift. Daten und Anwendungen werden nicht vom Gerät gelöscht.	Klicken Sie in der Dropdown-Liste **Erzwingungsaktion** auf **Quarantäne** (BlackBerry 10) oder **Nicht vertrauen** (iOS oder Android).
Löschen Sie die Geschäftsdaten vom Gerät.	Klicken Sie in der Dropdown-Liste **Erzwingungsaktion** auf **Nur Geschäftsdaten löschen**.
Löschen Sie alle Geschäftsdaten vom Gerät. Auf Geräten, auf denen „Geschäftlich und persönlich – Unternehmen“ oder „Geschäftlich und persönlich – Benutzer-Datenschutz“ aktiviert ist, werden nur Geschäftsdaten gelöscht.	Klicken Sie in der Dropdown-Liste **Erzwingungsaktion** auf **Alle Daten löschen**.

6. Wiederholen Sie die Schritte 4 und 5 für jeden Gerätetyp, für den Sie die Kompatibilitätsbedingungen konfigurieren möchten.
7. Wenn Sie Benutzern bei einem nicht konformen Gerät eine Benachrichtigung senden möchten, führen Sie eine der folgenden Aktionen aus:
    - Zum Ändern der E-Mail-Benachrichtigung erweitern Sie **Gesendete E-Mail-Benachrichtigung bei Erkennung einer Verletzung**. Ändern Sie den Betreff und die Nachricht.
    - Zum Ändern der Gerätebenachrichtigung erweitern Sie **Gesendete Gerätebenachrichtigung bei Erkennung einer Verletzung**. Ändern Sie die Nachricht.

    Wenn Sie Variablen zum Ausfüllen von Benachrichtigungen mit Benutzer-, Geräte- und Kompatibilitätsinformationen verwenden möchten, finden Sie weitere Informationen unter „Verwenden von Variablen“. Sie können auch eigene benutzerdefinierte Variablen mithilfe der Verwaltungskonsole definieren und verwenden. Weitere Informationen finden Sie unter „Benutzerdefinierte Variablen“.
8. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Legen Sie eine Rangfolge für die Kompatibilitätsprofile fest.

Verwandte Informationen
Verwenden von Variablen, auf Seite 64
Benutzerdefinierte Variablen, auf Seite 66

Filtern von Webinhalten auf iOS-Geräten

Sie können mithilfe von Webinhaltsfilter-Profilen die Webseiten einschränken, die ein Benutzer in Safari oder in anderen Browser-Apps auf einem iOS-Gerät aufrufen kann. Bei iOS-Geräten mit Secure Work Space begrenzen die Webinhaltsfilter-

Profile auch die Webseiten, die ein Benutzer in einem geschäftlichen Browser anzeigen kann. Sie können den Benutzerkonten, den Benutzergruppen oder den Gerätegruppen Webinhaltsfilter-Profile zuweisen.

Wenn Sie ein Webinhaltsfilter-Profil erstellen, können Sie die Option der zulässigen Webseiten auswählen, die die Normen Ihrer Organisation in Bezug auf die Nutzung von Mobilgeräten unterstützt.

Hinweis: Dieses Profil gilt nur für überwachte iOS-Geräte.

Zugelassene Websites	Beschreibung
Nur bestimmte Websites	Diese Option erlaubt nur den Zugriff auf die von Ihnen festgelegten Websites. Für jede zugelassene Website wird in Safari ein Lesezeichen erstellt.
Nicht jugendfreie Inhalte beschränken	Mit dieser Option werden unangemessene Inhalte automatisch erkannt und blockiert. Mit den folgenden Einstellungen können Sie auch bestimmte Websites einbinden: • Erlaubte URLs: Sie können eine oder mehrere URLs hinzufügen, um den Zugriff auf bestimmte Websites zu erlauben. Die Benutzer können die auf dieser Liste aufgeführten Websites unabhängig davon aufrufen, ob die automatische Filterung den Zugriff blockiert. • Gesperrte URLs: Sie können eine oder mehrere URLs hinzufügen, um den Zugriff auf bestimmte Websites zu sperren. Die Benutzer können die auf dieser Liste aufgeführten Websites nicht aufrufen, und zwar unabhängig davon, ob die automatische Filterung den Zugriff erlaubt.

Erstellen von Webinhaltsfilter-Profilen

Wenn Sie ein Webinhaltsfilter-Profil erstellen, muss jede von Ihnen festgelegte URL mit http:// oder https:// beginnen. Ggf. sollten Sie für http:// und https:// separate Eintragsversionen der gleichen URL hinzufügen. Da keine DNS-Auflösung erfolgt, ist es möglich, dass beschränkte Websites nach wie vor aufgerufen werden können (wenn Sie beispielsweise http://www.beispiel.com angeben, könnten die Benutzer dennoch über die IP-Adresse auf die Website zugreifen).

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf + neben **Webinhaltsfilter**.
3. Geben Sie einen Namen und eine Beschreibung für das Webinhaltsfilter-Profil ein.
4. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Einrichten des Zugriffs auf lediglich bestimmte Websites	1. Vergewissern Sie sich, dass in der Dropdown-Liste **Zugelassene Websites** die Option **Nur bestimmte Websites** ausgewählt ist. 2. Klicken Sie im Abschnitt **Lesezeichen für bestimmte Websites** auf +.

Aufgabe	Schritte
	3. Führen Sie folgende Aktionen aus: a Geben Sie im Feld **URL** eine Webadresse ein, für die der Zugriff gestattet werden soll. b Optional können Sie auch im Feld **Lesezeichenpfad** den Namen eines Lesezeichen-Ordners eingeben (zum Beispiel: /Work/). c Geben Sie im Feld **Titel** einen Namen für die Website ein. d Klicken Sie auf **Hinzufügen**. 4. Wiederholen Sie die Schritte 2 und 3 für alle zugelassenen Websites.
Nicht jugendfreie Inhalte beschränken	1. Klicken Sie in der Dropdown-Liste **Zugelassene Websites** auf **Nicht jugendfreie Inhalte beschränken**, um die automatische Filterung zu aktivieren. 2. Führen Sie optional folgende Aktionen aus: a Klicken Sie auf + neben **Erlaubte URLs**. b Eine Webadresse eingeben, für die der Zugang gewährt werden soll. c Für jede zugelassene Website die Schritte 2.a und 2.b wiederholen. 3. Führen Sie optional folgende Aktionen aus: a Klicken Sie auf + neben **Gesperrte URLs**. b Eine Webadresse eingeben, für die der Zugang verweigert werden soll. c Für jede eingeschränkte Website die Schritte 3.a und 3.b wiederholen.

5. Klicken Sie auf **Hinzufügen**.

Begrenzung von Geräten auf eine einzelne App

Auf überwachten iOS-Geräten oder Android-Geräten, die mit KNOX MDM verwaltet werden, können Sie mithilfe eines App-Sperrmodus-Profils erreichen, dass auf den Geräten nur eine einzige App ausgeführt werden kann. Beispielsweise können Sie ein Gerät zu Schulungszwecken oder für Vorführungen am Verkaufsort auf eine einzige App beschränken. Bei iOS-Geräten ist die Taste „Home“ deaktiviert, und das Gerät öffnet die App automatisch, wenn der Benutzer das Gerät aktiviert oder neu startet.

Erstellen eines Profils für den App-Sperrmodus

Wählen Sie eine App und die Geräteeinstellungen aus, die Sie für den Benutzer aktivieren möchten. Sie können bei iOS-Geräten eine App in der App-Liste auswählen, die Bundle-ID der App angeben oder eine integrierte App auswählen. Geben Sie bei Android-Geräten, die mit KNOX MDM verwaltet werden, den App-Paketbezeichner an, den Sie als Startseite festlegen möchten.

Hinweis: Wenn der Benutzer die App auf keinem Gerät installiert, dann ist das Gerät nach Zuweisung des Profils zu einem Benutzer oder einer Benutzergruppe nicht auf diese App beschränkt.

Bevor Sie beginnen: iOS-Geräte: Wenn Sie beabsichtigen, die App-Liste zur Auswahl einer App zu verwenden, sollten Sie sicherstellen, dass die App auch in der App-Liste verfügbar ist.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf + neben **App-Sperrmodus**.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
4. Legen Sie fest, ob das Profil auf iOS-Geräte, Android-Geräte oder auf beide Geräte angewandt werden soll.
5. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Festlegen der App, die auf iOS-Geräten ausgeführt werden soll	Führen Sie im Abschnitt **Die auf dem Gerät auszuführende App festlegen** eine der folgenden Aktionen aus: • Klicken Sie auf **Hinzufügen einer App**, und klicken Sie anschließend auf eine App in der Liste. • Klicken Sie auf **Die Bundle-ID einer App festlegen**, und geben Sie die Bundle-ID ein (zum Beispiel <*com.company.appname*>). Gültige Zeichen sind Groß- und Kleinbuchstaben, die Ziffern 0 bis 9, Bindestrich (-) und Punkt (.). • Klicken Sie auf **Eine integrierte iOS-App auswählen**, und wählen Sie eine App aus der Dropdown-Liste aus.
Festlegen der App, die auf Android-Geräten ausgeführt werden soll	Geben Sie im Feld **Die auf dem Gerät auszuführende App festlegen** den App-Paketbezeichner an, den Sie als Startseite festlegen möchten. Beispiel: Wenn als App „BBM Meetings“ verwendet werden soll, geben Sie **com.blackberry.bbm.meetings** ein.

6. Wählen Sie unter **Vom Administrator freigegebene Einstellungen** die Optionen aus, die Sie für den Benutzer bei Verwendung der App aktivieren möchten.
7. iOS-Geräte: Wählen Sie unter **Vom Benutzer aktivierbare Einstellungen** die Optionen aus, die der Benutzer aktivieren kann.
8. Klicken Sie auf **Hinzufügen**.

Steuern der Softwareversionen, die Benutzer auf BlackBerry 10-Geräten installieren können

Bei Geräten, auf denen BlackBerry 10 OS-Version 10.3.1 oder höher ausgeführt wird und die mit Geschäftlich und persönlich – Reguliert oder Nur geschäftlicher Bereich aktiviert werden, können Sie mit einem Profil für Gerätedienstanforderungen begrenzen, welche Softwareversionen auf BlackBerry 10-Geräten installiert werden können. Darüber hinaus können Sie für bestimmte Gerätemodelle Ausnahmen zu den globalen Einstellungen hinzufügen.

Um eine bestimmte Aktion zu erzwingen, wenn eine gesperrte Softwareversion auf einem Gerät installiert wird, müssen Sie ein Kompatibilitätsprofil erstellen und dieses Benutzern, Benutzergruppen oder Gerätegruppen zuweisen. Das Kompatibilitätsprofil gibt an, welche Aktionen ausgeführt werden, wenn der Benutzer die gesperrte Softwareversion nicht vom Gerät löscht.

Schritte zum Verwalten von Profilen für Gerätedienstanforderungen

Zum Verwalten von Profilen für Gerätedienstanforderungen führen Sie die folgenden Schritte aus:

Schritt	Aktion
1	Erstellen Sie das Profil.
2	Erstellen oder bearbeiten Sie ein Kompatibilitätsprofil, das die Aktionen angibt, die ausgeführt werden, wenn eine gesperrte Softwareversion auf einem Gerät installiert wird.
3	Weisen Sie dem Profil bei Bedarf eine Rangordnung zu.
4	Weisen Sie das Profil bei Bedarf zu.

Erstellen eines Profils für Gerätedienstanforderungen

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf + neben **Gerätedienstanforderungen**.
3. Um eine Liste aller BlackBerry 10-Softwareversionen des Geräts und entsprechender Informationen zu Betreiber, Gerätemodell, Hardware-ID, Softwareversion und Widerrufstatus anzuzeigen, klicken Sie auf **Anzeige einer Liste der Softwareversionen des Geräts**.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
5. Aktivieren Sie das Kontrollkästchen **Update erforderlich machen**, um eine Aktualisierung des Geräts auf eine im Profil definierte Softwareversion durch den Benutzer zu erzwingen.

6. Geben Sie im Feld **Übergangsfrist** einen Wert in Stunden ein, der verstreichen kann, bevor die Geräte zwingend aktualisiert werden müssen. Wenn Benutzer ihre Geräte innerhalb der Übergangsfrist nicht aktualisieren, oder wenn Sie die Übergangsfrist auf 0 setzen, wird das Softwareupdate automatisch auf den Geräten installiert.
7. Wählen Sie in der Dropdown-Liste **Mindestens erforderliche Softwareversion** die Softwareversion aus, die mindestens auf einem BlackBerry 10-Gerät ausgeführt werden muss.
8. Wählen Sie in der Dropdown-Liste **Maximale Softwareversion** die maximale Softwareversion aus, die auf einem BlackBerry 10-Gerät ausgeführt werden muss.
9. Um die globalen Einstellungen für ein Gerätemodell zu überschreiben, führen Sie die folgenden Aufgaben aus:
   a. Klicken Sie in der Tabelle **Ausnahmen** auf +.
   b. Wählen Sie in der Dropdown-Liste **Verfügbarkeit** aus, ob Sie Softwareversionen zulassen oder nicht zulassen möchten. Wenn Sie einen nicht zulässigen Bereich angeben und keinen zulässigen Bereich für ein Gerätemodell angegeben haben, wird eine zweite Spalte eingeblendet, in der Sie einen zulässigen Bereich angeben müssen. Wenn kein zulässiger Bereich angegeben wird, gelten die globalen Einstellungen nicht mehr für das Gerätemodell, und alle Softwareversionen, abgesehen von Ausnahmen, werden automatisch zugelassen.
   c. Wählen Sie in der Dropdown-Liste **Gerätemodell** das Gerätemodell aus, für das Sie eine Ausnahme einrichten möchten.
   d. Wählen Sie in der Dropdown-Liste **Mindestens** die mindestens erforderliche Softwareversion aus, die Sie zulassen oder nicht zulassen möchten.
   e. Wählen Sie in der Dropdown-Liste **Maximum** die maximale Softwareversion aus, die Sie zulassen oder nicht zulassen möchten.
   f. Wenn Sie eine Softwareversion nicht zugelassen haben, wählen Sie die mindestens erforderliche Softwareversion aus, die Sie zulassen möchten.
   g. Wenn Sie eine Softwareversion nicht zugelassen haben, wählen Sie die maximale Softwareversion aus, die Sie zulassen möchten.
10. Klicken Sie auf **Speichern**.
11. Klicken Sie auf **Hinzufügen**.

Benutzer anzeigen, die eine widerrufene Softwareversion ausführen

Sie können eine Liste von Benutzern anzeigen, die eine widerrufene Softwareversion ausführen. Bei einer widerrufenen Softwareversion handelt es sich um eine Softwareversion, die von einem Dienstanbieter nicht mehr akzeptiert wird, aber möglicherweise noch auf dem Gerät eines Benutzers installiert ist.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Erweitern Sie im linken Fensterbereich den Bereich **Gerätedienstanforderungen**.
3. Klicken Sie auf den Namen des Profils, das Sie anzeigen möchten.

4. Klicken Sie auf die Registerkarte **{0} Benutzer mit einer gesperrten Softwareversion**, um die Liste von Benutzern anzuzeigen, die eine widerrufene Softwareversion ausführen.

Verwalten von E-Mail- und Webdomänen für iOS 8-Geräte

Sie können ein Profil für verwaltete Domänen erstellen, um verwaltete E-Mail- und Webdomänen für iOS-Geräte zu definieren, auf denen iOS 8 oder höher ausgeführt wird.

Hinweis: Ein solches Profil wird nur auf Geräte angewendet, wenn diese mit einer MDM-Steuerelemente-Aktivierungsart aktiviert wurden.

In der folgenden Tabelle werden die Auswirkung des Hinzufügens von E-Mail- und Webdomänen in einem solchen Profil beschrieben:

Art der Domäne	Beschreibung
E-Mail-Domäne	E-Mail-Domänen, die im Profil der verwalteten Domänen aufgeführt sind, werden als unternehmensinterne Domänen betrachtet. Wenn ein Benutzer eine E-Mail von einem iOS 8-Gerät an eine E-Mail-Domäne sendet, die im Profil der verwalteten Domänen nicht aufgeführt ist, wird der Benutzer durch die Darstellung der E-Mail-Adresse in Rot gewarnt, dass es sich um einen unternehmensexternen Empfänger handelt. Das Gerät verhindert nicht, dass der Benutzer E-Mails an externe Empfänger sendet.
Webdomäne	Webdomänen, die im Profil der verwalteten Domänen aufgeführt sind, werden als unternehmensinterne Domänen betrachtet. Dokumente, die auf einer verwalteten Webdomäne angezeigt oder von dieser heruntergeladen werden, können nur auf dem iOS 8-Gerät unter Verwendung einer verwalteten App geöffnet werden. Das Gerät verhindert nicht, dass der Benutzer Dokumente auf anderen Webdomänen sucht oder anzeigt.

Erstellen eines Profils für verwaltete Domänen

Bevor Sie beginnen:

- Profile für verwaltete Domänen gelten nur für iOS-Geräte, auf denen iOS 8 oder höher ausgeführt wird.
- Profile für verwaltete Domänen gelten nur für Geräte mit der MDM-Steuerelemente-Aktivierungsart.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf + neben **Verwaltete Domänen**.
3. Geben Sie im Feld **Name** einen Namen für das Profil ein.

4. Geben Sie im Feld **Beschreibung** eine Beschreibung für das Profil ein.
5. Klicken Sie im Abschnitt **Verwaltete E-Mail-Domänen** auf +.
6. Geben Sie im Feld **E-Mail-Domäne** den Namen einer Domäne ein.
   Verwenden Sie nur den Namen der Domäne auf oberster Ebene. Verwenden Sie zum Beispiel `example.com` anstatt `example.com/canada`.
7. Klicken Sie auf **Hinzufügen**.
8. Klicken Sie im Abschnitt **Verwaltete Webdomänen** auf +.
9. Geben Sie im Feld **Webdomäne** den Namen einer Domäne ein.
10. Klicken Sie auf **Hinzufügen**.
11. Klicken Sie auf **Hinzufügen**.

Konfigurieren von zugelassenen und gesperrten Domänen auf Geräten mit einem geschäftlichen Bereich

Um einen Datenverlust zu verhindern, können Sie die Domänen konfigurieren, auf die die Benutzer über E-Mail, Kalender und Terminplanerdaten im geschäftlichen Bereich auf iOS- und Android-Geräten zugreifen können.

- Wenn Sie eine Liste an zugelassenen Domänen konfigurieren, können Benutzer uneingeschränkt auf die zugelassenen Domänen zugreifen. Sie können zum Beispiel auf Links zur Domäne klicken oder Empfängern über E-Mail-Adressen der Domäne hinzufügen, um E-Mails oder Kalendereinladungen zu senden. Befindet sich eine bestimmte Domäne nicht in der Liste der zugelassen Domänen, zeigt die App eine Warnmeldung an, wenn ein Benutzer versucht, auf eine solche Domäne zuzugreifen. Wenn der Benutzer auf OK tippt, kann er auf die Domäne zugreifen.
- Wenn Sie eine Liste an gesperrten Domänen konfigurieren, können Benutzer auf keine der Domänen in dieser Liste zugreifen. Wenn sie auf Links zur Domäne klicken oder versuchen, Empfänger über E-Mail-Adressen der Domäne hinzuzufügen, zeigt die App eine Fehlermeldung an und gestattet es dem Benutzer nicht, die Aufgabe abzuschließen. Ein Benutzer kann auf Domänen zugreifen, die sich nicht in der Liste mit gesperrten Domänen befinden.

Hinweis: Bei BlackBerry 10-Geräten können Sie alle zugelassenen und gesperrten Domänen mithilfe der IT-Richtlinien „Liste an zugelassenen externen E-Mail-Domänen“ und „Liste an gesperrten externen E-Mail-Domänen“ konfigurieren. Weitere Informationen finden Sie in der Richtlinien-Referenztabelle unter help.blackberry.com/detectLang/bes12/current/policy-reference-spreadsheet-zip/.

Konfigurieren von zugelassenen und gesperrten Domänen im geschäftlichen Bereich

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf das E-Mail-Profil, das Sie ändern möchten.
3. Klicken Sie auf .
4. Klicken Sie auf die Registerkarte **iOS** oder **Android**.
5. Fügen Sie im Abschnitt **Externe E-Mail-Domänen** die Domänen hinzu, die Sie zulassen möchten und die Domänen, die Sie einschränken möchten. Weitere Informationen finden Sie unter „iOS: E-Mail-Profileinstellungen“ oder „Android: E-Mail-Profileinstellungen“.
6. Klicken Sie auf **Speichern**.

Verwandte Informationen
iOS: E-Mail-Profileinstellungen, auf Seite 342
Android: E-Mail-Profileinstellungen, auf Seite 346

Erstellen von Organisationshinweisen zur Anzeige auf BlackBerry 10-Geräten

Sie können BES12 so konfigurieren, dass auf den BlackBerry 10-Geräten benutzerdefinierte Organisationshinweise angezeigt werden. Beispielsweise können Sie während einer Aktivierung festlegen, dass die Bedingungen angezeigt werden, die ein Benutzer befolgen muss, um die Sicherheitsanforderungen in Ihrer Organisation zu erfüllen. Der Benutzer muss den Hinweis bestätigen, um fortfahren zu können. Sie können mehrere Hinweise erstellen und so verschiedene Anforderungen abdecken. Darüber hinaus können Sie auch separate Versionen der einzelnen Hinweise erstellen, um verschiedene Sprachen zu unterstützen.

Bei Geräten, auf denen eine BlackBerry 10 OS-Version ab 10.3.1 läuft, können Sie auch BES12 konfigurieren, damit ein Organisationshinweis erscheint, sobald ein Benutzer ein Gerät neu startet.

Wann soll der Organisationshinweis angezeigt werden	Wie wird der Organisationshinweis konfiguriert
Bei der Aktivierung	Erstellen Sie einen Organisationshinweis, und weisen Sie ihn einem Aktivierungsprofil zu. Um den Hinweis zu ändern, der während der Aktivierung angezeigt wird, müssen Sie das Aktivierungsprofil aktualisieren und anschließend das Gerät neu aktivieren.
Beim Geräteneustart	Erstellen Sie einen Organisationshinweis, und weisen Sie ihn einem Geräteprofil zu. Vergewissern Sie sich, dass die IT-Richtlinie „Organisationshinweis nach Geräteneustart anzeigen“ ausgewählt wurde. Um den Hinweis zu ändern, der beim Geräteneustart angezeigt wird, müssen Sie das Geräteprofil aktualisieren.

Wann soll der Organisationshinweis angezeigt werden	Wie wird der Organisationshinweis konfiguriert
	Hinweis: Die IT-Richtlinie gilt nur für die Aktivierungsarten „Nur Geschäftlich“ und „Geschäftlich und persönlich – Reguliert“ auf Geräten, auf denen die BlackBerry 10 OS-Version 10.3.1 oder höher läuft.

Erstellen von Organisationshinweisen

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Erweitern Sie im linken Fensterbereich die Option **Allgemeine Einstellungen**.
3. Klicken Sie auf **Organisationshinweise**.
4. Klicken Sie am rechten Bildschirmrand auf +.
5. Geben Sie im Feld **Name** einen Namen für den Organisationshinweis ein.
6. Optional können Sie auch den Text aus einem bereits vorhandenen Organisationshinweis übernehmen, indem Sie ihn in der Dropdown-Liste **Kopierter Text aus Organisationshinweis** auswählen.
7. Wählen Sie in der Dropdown-Liste **Gerätesprache** die Sprache aus, die für den Organisationshinweis als Standardsprache verwendet werden soll.
8. Geben Sie im Feld **Organisationshinweis** den Text des Organisationshinweises ein.
9. Optional können Sie mehrmals auf **Hinzufügen einer weiteren Sprache** klicken, um den Organisationshinweis in mehreren Sprachen zu posten.
10. Wenn Sie den Organisationshinweis in mehr als einer Sprache posten, können Sie mithilfe der Option **Standardsprache** festlegen, welche standardmäßig verwendet wird.
11. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind:

- Wenn der Organisationshinweis während der Aktivierung angezeigt werden soll, weisen Sie den Organisationshinweis einem Aktivierungsprofil zu.
- Wenn der Organisationshinweis während eines Geräteneustarts angezeigt werden soll, weisen Sie den Organisationshinweis einem Geräteprofil zu.

Anzeigen von Organisationsinformationen auf Geräten

Sie können Geräteprofile zum Anzeigen von Informationen zu Ihrem Unternehmen auf BlackBerry 10-, iOS- und Android-Geräten erstellen.

Wenn Sie ein Geräteprofil erstellen, können Sie Organisationshinweise auf BlackBerry 10-, iOS- und Android-Geräten anzeigen lassen. Bei BlackBerry 10-Geräten wird ein Organisationshinweis angezeigt, wenn der Benutzer das Gerät neu startet. Bei iOS- und Android-Geräten werden die Informationen auf dem BES12 Client angezeigt.

Auf BlackBerry 10-Geräten können Sie ein benutzerdefiniertes Hintergrundbild für den geschäftlichen Bereich mit Informationen für die Benutzer hinzufügen. Sie können beispielsweise ein Bild erstellen, das Kontaktinformationen für den Support, Informationen zu einer internen Website oder das Logo Ihres Unternehmens enthält.

Erstellen eines Geräteprofils

Bevor Sie beginnen: Erstellen Sie Organisationshinweise für BlackBerry 10-Geräte.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf + neben **Gerät**.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein. Jedes Geräteprofil muss über einen eindeutigen Namen verfügen.
4. Führen Sie zum Hinzufügen eines Organisationshinweises eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Zuweisen eines Organisationshinweises zur Anzeige auf BlackBerry 10-Geräten während des Geräteneustarts	1. Klicken Sie auf **BlackBerry**. 2. Wählen Sie in der Dropdown-Liste **Organisationshinweis zuweisen** den Organisationshinweis aus, der auf Geräten angezeigt werden soll.
Definieren der Organisationsinformationen zur Anzeige auf dem BES12 Client für iOS- oder Android-Geräte	1. Klicken Sie auf **iOS** oder **Android**. 2. Geben Sie den Namen, die Adresse, Telefonnummer und E-Mail-Adresse Ihrer Organisation ein.

5. Führen Sie zum Hinzufügen eines Hintergrundbilds zum geschäftlichen Bereich auf BlackBerry 10-Geräten die folgenden Aufgaben aus:
   a. Klicken Sie auf **BlackBerry**.
   b. Klicken Sie im Bereich **Hintergrundbild für den geschäftlichen Bereich** auf **Durchsuchen**.
   c. Wählen Sie das gewünschte Bild aus.
   d. Klicken Sie auf **Öffnen**.
6. Klicken Sie auf **Hinzufügen**.

Erstellen von Websymbolen für iOS-Geräte

Sie können mit einem Websymbol-Profil ein benutzerdefiniertes Websymbol zur Anzeige auf den Geräten der Benutzer erstellen. Sie können z. B. ein benutzerdefiniertes Websymbol erstellen, das als Verknüpfung zur internen Website Ihres Unternehmens fungiert. Für jedes Websymbol-Profil können Sie die folgenden Attribute konfigurieren:

- Webadresse, die geöffnet wird, wenn Benutzer auf das Websymbol tippen.
- Erscheinungsbild des Websymbols, d. h. Bild und Beschriftung
- Ob Benutzer das Websymbol von ihren Geräten entfernen können
- Ob die Webadresse im Vollbildmodus auf den Geräten der Benutzer geöffnet wird

Erstellen von Websymbol-Profilen

Sie müssen ein Websymbol-Profil für jedes Websymbol erstellen, das auf Geräten der Benutzer angezeigt werden soll. Wenn ein Benutzer ein Websymbol von einem Gerät entfernt und es wiederherstellen möchte, müssen Sie das Websymbol-Profil entfernen und dem Benutzer neu zuweisen. Wenn Sie das Kontrollkästchen „Websymbol als Vollbild-App öffnen“ deaktivieren, wird die Webadresse in einem Browser geöffnet.

Hinweis: Websymbol-Profile werden auf Geräten mit der Aktivierungsart „Geschäftlich und persönlich – Benutzer-Datenschutz“ nicht unterstützt.

Bevor Sie beginnen: Das Bild, das Sie für das Websymbol verwenden möchten, muss folgende Anforderungen erfüllen:

- Das Bildformat muss .png, .jpg oder .jpeg sein.
- Vermeiden Sie PNG-Bilder mit transparenten Elementen. Transparente Elemente werden auf Geräten schwarz angezeigt.
- Informationen zur empfohlenen Bildgröße finden Sie unter „Icon and Image Sizes“ auf der Website developer.apple.com.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf + neben dem **Websymbol**.
3. Geben Sie einen Namen und eine Beschreibung für das Websymbol-Profil ein. Dieser Name wird als Beschriftung für das Websymbol verwendet.
4. Klicken Sie auf **Durchsuchen**. Wählen Sie das Bild für das Websymbol aus. Es werden die Bildformate .png, .jpg und .jpeg unterstützt.
5. Geben Sie im Feld **URL** die Webadresse ein, die geöffnet werden soll, wenn Benutzer auf das Websymbol tippen. Die Webadresse muss mit „http://“ oder „https://“ beginnen. Bei Geräten mit der Aktivierungsart „Geschäftlich und persönlich – vollständige Kontrolle“ können Sie eine Webadresse, die mit „sec-connect://“ oder „sec-connects://“ beginnt, zum Öffnen der Website im Browser des geschäftlichen Bereichs verwenden.
6. Sollen Benutzer das Websymbol von der Startseite ihres Gerät entfernen können, aktivieren Sie das Kontrollkästchen **Entfernen durch Benutzer zulassen**.

7. Soll die Webadresse im Vollbildmodus auf den Geräten der Benutzer geöffnet werden, aktivieren Sie das Kontrollkästchen **Websymbol als Vollbild-App öffnen**.
8. Klicken Sie auf **Hinzufügen**.

Einrichten der Standortbestimmung für iOS-Geräte

Sie können eine Standortbestimmung in BES12 einrichten, mit deren Hilfe Sie oder Benutzer iOS-Geräte auf einer Karte orten können.

Schritte zur Einrichtung von Profilen für die Standortbestimmung

Beim Einrichten von Profilen für die Standortbestimmung führen Sie die folgenden Aktionen aus:

Schritt	Aktion
1	Profil für die Standortbestimmung erstellen und bearbeiten
2	Zuweisen des Profils für die Standortbestimmung zu einem Benutzer, einer Benutzergruppe oder einer Gerätegruppe

Erstellen von Profilen für die Standortbestimmung

Profile für die Standortbestimmung ermöglichen Benutzern von iOS-Geräten das Orten ihres Gerät mithilfe von BES12 Self-Service. Der Standort des Gerätes wird auf einer Karte in der Verwaltungskonsole oder in BES12 Self-Service angezeigt.

Nach der Erstellung eines Profils für die Standortbestimmung können Sie dieses Benutzern, Benutzergruppen oder Gerätegruppen zuweisen. Es gibt kein Standardprofil für die Standortbestimmung.

Hinweis: Benutzer müssen das Profil für die Standortbestimmung akzeptieren, damit der Standort ihres Geräts in der Verwaltungskonsole oder BES12 Self-Service angezeigt werden kann.

Erstellen eines Profils für die Standortbestimmung

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie im linken Fensterbereich auf + neben **Standortbestimmung**.
3. Geben Sie einen Namen und eine Beschreibung für das Profil für die Standortbestimmung ein.

4. Wenn Sie zulassen möchten, dass Benutzer ihre iOS-Geräte in BES12 Self-Service orten können, aktivieren Sie das Kontrollkästchen **Dienst für die Standortbestimmung in der Selbstbedienungskonsole aktivieren**.
5. Aktivieren Sie das Kontrollkästchen **Gerätetypen anzeigen für die Konfiguration des Profils für**.
6. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind:

- Weisen Sie das Profil Benutzerkonten, Benutzergruppen oder Gerätegruppen zu.
- Wenn Sie mehrere Profile für die Standortbestimmung erstellen, weisen Sie ihnen eine Rangordnung zu.

Nach der Zuweisung eines Profils für die Standortbestimmung erhalten die Benutzer eine Aufforderung auf ihren iOS-Geräten, die Standortbestimmung zuzulassen. Wenn die Benutzer diese Aufforderung nicht akzeptieren, kann ihr iOS-Gerät nicht geortet bzw. auf einer Karte angezeigt werden.

Sie können in der Verwaltungskonsole auf einen Benutzernamen klicken, um festzustellen, ob der Benutzer das Profil für die Standortbestimmung auf seinem iOS-Gerät akzeptiert hat.

IT-Richtlinien

Verwenden Sie IT-Richtlinien zur Verwaltung der Sicherheit und des Verhaltens von Geräten.

Secure

Steuern von Gerätefunktionen mithilfe von IT-Richtlinien

18

Sie können IT-Richtlinien zum Verhalten der Sicherheit und des Verhaltens von Geräten in Ihrer Organisation verwenden. Eine IT-Richtlinie ist ein Regelsatz, mit dem Funktionen und die Funktionalität von Geräten gesteuert werden. Sie können Regeln für BlackBerry 10-, iOS-, Android- und Windows Phone-Geräte in derselben IT-Richtlinie konfigurieren.

BES12 enthält eine Standard-IT-Richtlinie mit vorkonfigurierten Regeln für jeden Gerätetyp. Wenn einem Benutzerkonto, einer Benutzergruppe, dem ein Benutzer angehört, oder einer Gerätegruppe, dem die Geräte eines Benutzers angehören, keine IT-Richtlinie zugewiesen ist, sendet BES12 die Standard-IT-Richtlinie an die Geräte des Benutzers. BES12 sendet automatisch eine IT-Richtlinie an ein Gerät, wenn es von einem Benutzer aktiviert wird, wenn Sie eine zugewiesene IT-Richtlinie aktualisieren oder wenn einem Benutzerkonto oder Gerät eine andere IT-Richtlinie zugewiesen wird.

BES12 wird täglich über Port 3101 mit BlackBerry Infrastructure synchronisiert, um zu bestimmen, ob aktualisierte IT-Richtlinieninformationen verfügbar sind. Wenn aktualisierte IT-Richtlinieninformationen verfügbar sind, werden sie von BES12 abgerufen und in der BES12-Datenbank gespeichert. Administratoren mit der Berechtigung „IT-Richtlinien anzeigen“ bzw. „IT-Richtlinien erstellen und bearbeiten“ werden über das Update benachrichtigt, wenn sie sich anmelden.

Schritte zum Verwalten von IT-Richtlinien

Um IT-Richtlinien zu verwalten, führen Sie die folgenden Aktionen aus:

Schritt	Aktion
1	Überprüfen Sie die Standard-IT-Richtlinie, und nehmen Sie bei Bedarf Aktualisierungen vor.
2	Legen Sie optional benutzerdefinierte IT-Richtlinien an.
3	Ggf. müssen Sie den IT-Richtlinien einen Rang zuweisen.
4	Wenn Sie benutzerdefinierte IT-Richtlinien erstellen, weisen Sie diese den Benutzerkonten, Benutzergruppen oder Gerätegruppen zu.

Einschränken und Zulassen von Gerätefunktionen

Bei der Konfiguration von IT-Richtlinienregeln können Sie Gerätefunktionen einschränken oder zulassen. Die für jeden Gerätetyp verfügbaren IT-Richtlinienregeln werden in der Regel vom Betriebssystem und der Version des Geräts bestimmt. Einige Regeln für iOS und Android werden von Optionen wie Secure Work Space und KNOX MDM bestimmt. Je nach Gerätetyp können Sie beispielsweise IT-Richtlinienregeln verwenden, um folgende Aufgaben zu erledigen:

- Durchsetzung von Kennwortanforderungen
- Verhindern, dass Benutzer die Gerätekamera verwenden
- Steuern von Verbindungen über die drahtlose Bluetooth-Technologie
- Steuern der Verfügbarkeit bestimmter Apps

Sie können IT-Richtlinien verwenden, um Gerätefunktionen, den geschäftlichen Bereich auf Geräten bzw. beides zu steuern. Die Geräteaktivierungsart und – falls zutreffend – Optionen wie Secure Work Space und KNOX MDM bestimmen, welche Regeln in der IT-Richtlinie auf das Gerät angewandt werden. Weitere Informationen zu IT-Richtlinienregeln für die einzelnen Gerätetypen finden Sie in der Richtlinien-Referenztabelle unter help.blackberry.com/detectlang/bes12/current/policy-reference-spreadsheet-zip/ .

So wählt BES12 die zuzuweisenden IT-Richtlinien aus

BES12 sendet nur eine IT-Richtlinie an ein Gerät und verwendet vordefinierte Regeln, um zu bestimmen, welche IT-Richtlinie einem Benutzer und den Geräten, die der Benutzer aktiviert, zugewiesen werden soll.

Zugewiesen zu	Regeln
Benutzerkonto (Registerkarte „Benutzerzusammenfassung“ anzeigen)	1. Eine IT-Richtlinie, die einem Benutzerkonto direkt zugewiesen wurde, hat Vorrang vor einer IT-Richtlinie, die indirekt über die Benutzergruppe zugewiesen wurde. 2. Wenn ein Benutzer Mitglied mehrerer Benutzergruppen mit verschiedenen IT-Richtlinien ist, weist BES12 die IT-Richtlinie mit der höchsten Rangordnung zu. 3. Die Standard-IT-Richtlinie wird zugewiesen, wenn einem Benutzerkonto keine IT-Richtlinie direkt oder durch die Mitgliedschaft in einer Benutzergruppe zugewiesen wird.
Gerät (Registerkarte „Gerät anzeigen“)	Standardmäßig erbt ein Gerät die IT-Richtlinie, die BES12 dem Benutzer zuweist, der das Gerät aktiviert. Wenn ein Gerät einer Gerätegruppe angehört, gelten die folgenden Regeln:

Zugewiesen zu	Regeln
	1. Eine IT-Richtlinie, die einer Gerätegruppe zugewiesen ist, hat Vorrang vor der IT-Richtlinie, die BES12 einem Benutzerkonto zuweist. 2. Wenn ein Gerät Mitglied mehrerer Gerätegruppen mit verschiedenen IT-Richtlinien ist, weist BES12 die IT-Richtlinie mit der höchsten Rangordnung zu.

BES12 muss unter Umständen in Konflikt stehende IT-Richtlinien auflösen, falls Sie eine der folgenden Aktionen ausführen:

- Zuweisen einer IT-Richtlinie zu einem Benutzerkonto, einer Benutzergruppe oder einer Gerätegruppe
- Entfernen einer IT-Richtlinie aus einem Benutzerkonto, einer Benutzergruppe oder einer Gerätegruppe
- Ändern der Rangordnung der IT-Richtlinien
- Löschen einer IT-Richtlinie
- Ändern der Zugehörigkeit in einer Benutzergruppe (Benutzerkonten und verschachtelte Gruppen)
- Ändern von Geräteattributen
- Ändern der Mitgliedschaft in einer Gerätegruppe
- Löschen einer Benutzergruppe oder Gerätegruppe

Verwandte Informationen
IT-Richtlinien einen Rang zuweisen, auf Seite 141

Erstellen und Verwalten von IT-Richtlinien

Sie können die Standard-IT-Richtlinie verwenden oder benutzerdefinierte IT-Richtlinien erstellen (um beispielsweise IT-Richtlinienregeln für verschiedene Benutzergruppen oder Gerätegruppen in Ihrem Unternehmen festzulegen). Wenn Sie vorhaben, die Standard-IT-Richtlinie zu verwenden, sollten Sie diese überprüfen und bei Bedarf aktualisieren, um sicherzustellen, dass die Regeln die Sicherheitsstandards Ihrer Organisation erfüllen.

Erstellen einer IT-Richtlinie

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf + neben **IT-Richtlinien**.
3. Geben Sie einen Namen und eine Beschreibung für die IT-Richtlinie ein.
4. Klicken Sie auf die Registerkarte für jeden Gerätetyp in Ihrem Unternehmen, und konfigurieren Sie die entsprechenden Werte für die IT-Richtlinienregeln.
5. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Weisen Sie IT-Richtlinien einen Rang zu.

Kopieren einer IT-Richtlinie

Sie können IT-Richtlinien zur schnellen Erstellung benutzerdefinierter IT-Richtlinien für verschiedene Gruppen in Ihrem Unternehmen kopieren.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Erweitern Sie im linken Fensterbereich die Option **IT-Richtlinien**.
3. Klicken Sie auf den Namen der IT-Richtlinie, die Sie kopieren möchten.
4. Klicken Sie auf .
5. Geben Sie einen Namen und eine Beschreibung für die neue IT-Richtlinie ein.
6. Nehmen Sie die gewünschten Änderungen für jeden Gerätetyp auf der entsprechenden Registerkarte vor.
7. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Weisen Sie IT-Richtlinien einen Rang zu.

IT-Richtlinien einen Rang zuweisen

Mithilfe der Rangordnung lässt sich festlegen, welche IT-Richtlinie in den folgenden Szenarien BES12 an ein Gerät sendet:

- Ein Benutzer ist Mitglied in mehreren Benutzergruppen, die unterschiedliche IT-Richtlinien aufweisen.
- Ein Gerät ist Mitglied in mehreren Gerätegruppen, die unterschiedliche IT-Richtlinien aufweisen.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Erweitern Sie im linken Fensterbereich den Bereich **IT-Richtlinien**.
3. Klicken Sie auf **IT-Richtlinien einen Rang zuweisen**.
4. Mit den Pfeiltasten können Sie die IT-Richtlinien in der Rangordnung nach oben oder unten verschieben.
5. Klicken Sie auf **Speichern**.

Verwandte Informationen

So wählt BES12 die zuzuweisenden IT-Richtlinien aus, auf Seite 139

Anzeigen einer IT-Richtlinie

Sie können die folgenden Informationen zu einer IT-Richtlinie anzeigen:

- IT-Richtlinienregeln, speziell für jeden Gerätetyp
- Liste und Anzahl der Benutzerkonten, denen die IT-Richtlinie zugewiesen ist (direkt und indirekt)
- Liste und Anzahl der Benutzergruppen, denen die IT-Richtlinie zugewiesen ist (direkt)

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Erweitern Sie im linken Fensterbereich den Bereich **IT-Richtlinien**.

3. Klicken Sie auf den Namen der IT-Richtlinie, die Sie anzeigen möchten.

Ändern einer IT-Richtlinie

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Erweitern Sie im linken Fensterbereich den Bereich **IT-Richtlinien**.
3. Klicken Sie auf den Namen der IT-Richtlinie, die Sie ändern möchten.
4. Klicken Sie auf .
5. Nehmen Sie für jeden Gerätetyp Änderungen in der jeweiligen Registerkarte vor.
6. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Ändern Sie bei Bedarf die IT-Richtlinienrangordnung.

Entfernen einer IT-Richtlinie aus den Benutzerkonten oder Benutzergruppen

Wenn eine IT-Richtlinie direkt den Benutzerkonten oder Benutzergruppen zugewiesen wurde, können Sie diese aus den Benutzern oder Gruppen entfernen. Wenn eine IT-Richtlinie indirekt durch die Benutzergruppe zugewiesen ist, können Sie die IT-Richtlinie oder die Benutzerkonten aus der Gruppe entfernen. Wenn Sie eine IT-Richtlinie aus den Benutzergruppen entfernen, wird die IT-Richtlinie aus jedem Benutzer entfernt, der den ausgewählten Gruppen angehört.

Hinweis: Die Standard-IT-Richtlinie kann nur dann aus einem Benutzerkonto entfernt werden, wenn Sie es dem Benutzer direkt zugewiesen haben.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Erweitern Sie im linken Fensterbereich den Bereich **IT-Richtlinien**.
3. Klicken Sie auf den Namen der IT-Richtlinie, die Sie aus den Benutzerkonten oder Benutzergruppen entfernen möchten.
4. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Entfernen einer IT-Richtlinie von Benutzerkonten	1. Klicken Sie auf die Registerkarte **Benutzern zugewiesen**. 2. Suchen Sie ggf. nach den Benutzerkonten. 3. Wählen Sie die Benutzerkonten aus, aus denen Sie die IT-Richtlinie entfernen möchten. 4. Klicken Sie auf .
Entfernen einer IT-Richtlinie von Benutzergruppen	1. Klicken Sie auf die Registerkarte **Gruppen zugewiesen**. 2. Suchen Sie ggf. nach den Benutzergruppen.

Aufgabe	Schritte
	3. Wählen Sie die Benutzergruppen aus, aus denen Sie die IT-Richtlinie entfernen möchten. 4. Klicken Sie auf .

Verwandte Informationen

So wählt BES12 die zuzuweisenden IT-Richtlinien aus, auf Seite 139

Löschen einer IT-Richtlinie

Sie können die Standard-IT-Richtlinie nicht löschen. Wenn Sie eine benutzerdefinierte IT-Richtlinie löschen, entfernt BES12 die IT-Richtlinie aus den Benutzern und deren verknüpften Geräten.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Erweitern Sie im linken Fensterbereich den Bereich **IT-Richtlinien**.
3. Klicken Sie auf den Namen der IT-Richtlinie, die Sie löschen möchten.
4. Klicken Sie auf .
5. Klicken Sie auf **Löschen**.

Verwandte Informationen

So wählt BES12 die zuzuweisenden IT-Richtlinien aus, auf Seite 139

Steuern von BlackBerry OS-Gerätefunktionen mithilfe von IT-Richtlinien

19

Wenn die BES12-Domäne BlackBerry OS-Geräte (Version 5.0 bis 7.1) unterstützt, können Sie die BlackBerry OS-IT-Richtlinien verwenden, um die BlackBerry OS-Geräte, die BlackBerry Desktop Software und den BlackBerry Web Desktop Manager in Ihrer Organisationsumgebung zu steuern und zu verwalten. Eine BlackBerry OS-IT-Richtlinie besteht aus mehreren IT-Richtlinienregeln zur Verwaltung der Sicherheit und des Verhaltens von BlackBerry OS-Benutzergeräten.

BES12 enthält vorkonfigurierte BlackBerry OS-IT-Richtlinien, einschließlich einer Standard-IT-Richtlinie, die IT-Richtlinienregeln enthält und die zum Darstellen des Standardverhaltens des BlackBerryOS-Geräts oder der BlackBerry Desktop Software konfiguriert sind. Wenn einem Benutzerkonto oder einer Benutzergruppe, der der Benutzer angehört, keine BlackBerry OS-IT-Richtlinie zugewiesen wurde, sendet BES12 die Standard-IT-Richtlinie an das BlackBerry OS-Gerät des Benutzers. BES12 sendet automatisch eine BlackBerry OS-IT-Richtlinie an ein Gerät, wenn sie ein Benutzer aktiviert, wenn Sie eine zugewiesene IT-Richtlinie aktualisieren oder wenn einem Benutzerkonto eine andere IT-Richtlinie zugewiesen wurde.

Schritte zum Verwalten von BlackBerry OS-IT-Richtlinien

Um BlackBerry OS-IT-Richtlinien zu verwalten, führen Sie die folgenden Aktionen aus:

Schritt	Aktion
1	Überprüfen Sie die vorkonfigurierten BlackBerry OS-IT-Richtlinien, einschließlich der Standard-IT-Richtlinie, und aktualisieren Sie sie bei Bedarf.
2	Legen Sie optional benutzerdefinierte BlackBerry OS-IT-Richtlinien an.
3	Legen Sie die Rangordnung der BlackBerry OS-IT-Richtlinien fest.
4	Weisen Sie Benutzerkonten oder Benutzergruppen vorkonfigurierte oder benutzerdefinierte BlackBerry OS-IT-Richtlinien zu.

Einschränken und Zulassen von BlackBerry OS-Gerätefunktionen

Mithilfe von IT-Richtlinienregeln können Sie die Aktionen, die die BlackBerry OS-Geräte (Version 5.0 bis 7.1) ausführen können, anpassen und steuern. Um eine IT-Richtlinienregel auf einem BlackBerry OS-Gerät verwenden zu können, müssen Sie sicherstellen, dass die BlackBerry Desktop Software-Version die IT-Richtlinienregel unterstützt. Je nach Version der BlackBerry Desktop Software können Sie beispielsweise IT-Richtlinienregeln verwenden, um folgende Aufgaben zu erledigen:

- Durchsetzung von Kennwortanforderungen
- Steuern von Verbindungen über die drahtlose Bluetooth-Technologie
- Schützen von Benutzerdaten und Gerätetransportschlüsseln auf dem Gerät
- Steuern der für Drittanbieteranwendungen verfügbaren Geräteressourcen, z. B. Kamera oder GPS

Weitere Informationen über die IT-Richtlinien für BlackBerry OS-Geräte finden Sie in der Richtlinien-Referenztabelle unter help.blackberry.com/detectLang/bes12/current/policy-reference-spreadsheet-zip/.

Vorkonfigurierte BlackBerry OS-IT-Richtlinien

Wenn die BES12 Domäne BlackBerry -Geräte (Version 5.0 bis 7.1) unterstützt, enthält BES12 die folgenden vorkonfigurierten BlackBerry OS-IT-Richtlinien, die Sie an die Anforderungen Ihrer Organisation anpassen können:

Vorkonfigurierte IT-Richtlinie	Beschreibung
Standard	Diese Richtlinie enthält alle standardmäßigen IT-Richtlinienregeln, die in BES12 festgelegt sind.
Geräte mit individueller Haftung	Ähnlich wie die Standard-IT-Richtlinie verhindert diese Richtlinie, dass BlackBerry OS-Gerätebenutzer auf ihren Geräten von Social Networking-Apps aus auf Kalenderdaten zugreifen. Diese Richtlinie lässt es zu, dass Benutzer auf ihre persönlichen Kalenderdienste und E-Mail-Nachrichtendienste zugreifen, die BlackBerry Device Software mit außerhalb Ihrer Organisation verfügbaren Methoden aktualisieren, Anrufe tätigen, wenn Geräte gesperrt sind, sowie Text ausschneiden, kopieren und einfügen. Benutzer können E-Mail-Nachrichten nicht von einem E-Mail-Nachrichtendienst an einen anderen weiterleiten. Sie können die IT-Richtlinie "Persönliche Gerätehaftung" verwenden, wenn es in Ihrer Organisation Benutzer gibt, die ihre eigenen Geräte erwerben und die Geräte mit einer BES12-Instanz in Ihrer Organisationsumgebung verbinden.
Einfache Kennwortsicherheit	Ähnlich wie die Standard-IT-Richtlinie erfordert diese Richtlinie ein einfaches Kennwort, mit dem Benutzer ihre Geräte entsperren können. Benutzer müssen die

Vorkonfigurierte IT-Richtlinie	Beschreibung
	Kennwörter regelmäßig ändern. Die IT-Richtlinie umfasst ein Kennwort-Timeout, das Geräte sperrt.
Mittlere Kennwortsicherheit	Ähnlich wie die Standard-IT-Richtlinie erfordert diese Richtlinie ein komplexes Kennwort, mit dem Benutzer ihre Geräte entsperren können. Benutzer müssen die Kennwörter regelmäßig ändern. Diese Richtlinie umfasst einen maximalen Kennwortverlauf und deaktiviert Bluetooth-Technologie auf Geräten.
Mittlere Sicherheit ohne Anwendungen von Drittanbietern	Ähnlich wie die Richtlinie für mittlere Kennwortsicherheit erfordert diese Richtlinie ein komplexes Kennwort, das Benutzer oft ändern müssen, ein Sicherheits-Timeout und einen maximalen Kennwortverlauf. Diese Richtlinie hindert Benutzer daran festzulegen, dass ihre Geräte von anderen Bluetooth-fähigen Geräten erkannt werden können, und verhindert, dass Geräte Anwendungen von Drittanbietern herunterladen.
Erhöhte Sicherheit	Ähnlich wie die Standard-IT-Richtlinie erfordert diese IT-Richtlinie ein komplexes Kennwort, das Benutzer häufig ändern müssen, ein Kennwort-Timeout zur Sperrung von Geräten und einen maximalen Kennwortverlauf. Diese Richtlinie schränkt Bluetooth-Technologie auf Geräten ein, aktiviert starken Inhaltsschutz, deaktiviert den USB-Massenspeicher und erfordert, dass Geräte externe Dateisysteme verschlüsseln.
Erhöhte Sicherheit ohne Anwendungen von Drittanbietern	Ähnlich wie die IT-Richtlinie „Erhöhte Sicherheit“ erfordert diese IT-Richtlinie ein komplexes Kennwort, das Benutzer häufig ändern müssen, ein Kennwort-Timeout zur Sperrung von Geräten und einen maximalen Kennwortverlauf. Diese Richtlinie schränkt Bluetooth-Technologie auf Geräten ein, aktiviert starken Inhaltsschutz, deaktiviert den USB-Massenspeicher, erfordert, dass Geräte externe Dateisysteme verschlüsseln, und verhindert, dass Geräte Anwendungen von Drittanbietern herunterladen.

Zuweisen von BlackBerry OS-IT-Richtlinien und Auflösen von Konflikten zwischen IT-Richtlinien

Wenn einem Benutzerkonto weder direkt noch über die Mitgliedschaft in einer Benutzergruppe eine BlackBerry OS-IT-Richtlinie zugewiesen wurde, wendet BES12 die Standard-IT-Richtlinie für das Benutzerkonto an. Eine BlackBerry OS-IT-Richtlinie, die einem Benutzerkonto direkt zugewiesen wurde, hat Vorrang vor einer IT-Richtlinie, die indirekt über die Benutzergruppe zugewiesen wurde.

Wenn ein Benutzerkonto Mitglied mehrerer Gruppen ist, für die unterschiedliche BlackBerry OS-IT-Richtlinien gelten, muss BES12 anhand einer der folgenden Methoden festlegen, welche BlackBerry OS-IT-Richtlinie auf das Benutzerkonto anzuwenden ist.

Methode	Beschreibung
Anwenden einer IT-Richtlinie auf das Benutzerkonto	BES12 wendet die ranghöchste BlackBerry OS-IT-Richtlinie auf das Benutzerkonto an.
Anwenden von mehreren IT-Richtlinien auf ein Benutzerkonto	BES12 kombiniert die BlackBerry OS-IT-Richtlinien, die jeder einzelnen Benutzergruppe zugewiesen sind, in einer IT-Richtlinie und weist sie dem Benutzerkonto zu, sodass eine kombinierte IT-Richtlinie mit einer individuellen ID entsteht. Wenn eine IT-Richtlinienregel von den mehrfachen BlackBerry OS-IT-Richtlinien abweicht, haben alle Regeleinstellungen, die explizit auf einen Wert konfiguriert worden sind, Vorrang vor den Regeleinstellungen der IT-Richtlinien, die leer sind (diese Regeln stellen den Standardwert wieder her). Andernfalls löst BES12 in Konflikt stehende Regeleinstellungen auf, indem die Regeleinstellung aus der ranghöchsten IT-Richtlinie angewendet wird.

BES12 muss unter Umständen in Konflikt stehende IT-Richtlinien auflösen, falls Sie eine der folgenden Aktionen ausführen:

- Zuweisen einer BlackBerry OS-IT-Richtlinie zu einem Benutzerkonto oder zu einer Benutzergruppe
- Entfernen einer BlackBerry OS-IT-Richtlinie aus einem Benutzerkonto oder aus einer Benutzergruppe
- Ändern der Rangordnung von BlackBerry OS-IT-Richtlinien
- Ändern einer BlackBerry OS-IT-Richtlinie
- Löschen einer BlackBerry OS-IT-Richtlinie
- Ändern der Zugehörigkeit in einer Benutzergruppe (Benutzerkonten und verschachtelte Gruppen)
- Löschen einer Benutzergruppe

Verwandte Informationen

Zuweisen eines Rangs zu BlackBerry OS-IT-Richtlinien, auf Seite 149

Ändern der Methode, die BES12 zum Auflösen in Konflikt stehender IT-Richtlinien verwendet

Sie können die Methode ändern, mit der BES12 feststellt, welche BlackBerry OS-IT-Richtlinie für ein Benutzerkonto gilt, wenn ein Benutzer Mitglied von mehreren Benutzergruppen mit verschiedenen BlackBerry OS-IT-Richtlinien ist. Wenn Sie die Methode ändern, die zum Auflösen von in Konflikt stehenden IT-Richtlinien oder IT-Richtlinieneinstellungen verwendet wird, kann sich die nächste Abstimmung der BlackBerry OS-IT-Richtlinie deutlich auf die Leistung Ihrer BES12-Organisationsumgebung auswirken. Es empfiehlt sich, diese Funktion in Zeiten niedriger Auslastung zu konfigurieren.

1. Klicken Sie in der Menüleiste auf **BlackBerry OS-Einstellungen**.
2. Erweitern Sie im Menü **Server und Komponenten** die Einträge **Topologie der BlackBerry-Lösung** > **BlackBerry Domain** > **Komponente: Anzeigen**.

3. Klicken Sie auf **BlackBerry Administration Service**.
4. Klicken Sie unten auf der Seite auf **Methode zum Auflösen mehrerer IT-Richtlinien ändern**.
5. Klicken Sie auf **Ja – Methode ändern**.

Deaktivieren von BlackBerry OS-Geräten, auf die keine IT-Richtlinien angewendet wurden

Um zu verhindern, dass BlackBerry OS-Geräte (Version 5.0 bis 7.1), auf die keine IT-Richtlinien angewendet wurden, unter BES12 aktiv bleiben, können Sie für die IT-Richtlinienoption „Benutzer ohne angewendete IT-Richtlinie deaktivieren“ den Wert „Wahr“ festlegen. Die Einstellung „Zeitraum bis zur Deaktivierung des Benutzers (Stunden)“ gibt den Zeitraum an, in dem die BlackBerry OS-Geräte unter BES12 aktiv bleiben können, ohne dass eine IT-Richtlinie auf die Geräte angewendet wird.

Wenn Sie den Wert für die Option „Benutzer ohne angewendete IT-Richtlinie deaktivieren“ in „Wahr“ ändern, sendet BES12 die BlackBerry OS-IT-Richtlinie standardmäßig alle 30 Minuten an die BlackBerry OS-Geräte, bis die Geräte die IT-Richtlinie anwenden oder die Zeitbeschränkung abläuft. Wenn die Zeitbeschränkung abläuft, deaktiviert BES12 die BlackBerry OS-Geräte-PINs. Der gültige Bereich für den Wert dieser Einstellung liegt zwischen 0 und 8760 Stunden. Wenn Sie 0 Stunden angeben, werden BlackBerry OS-Geräte deaktiviert, wenn die IT-Richtlinie nicht automatisch angewendet werden kann.

Deaktivieren von BlackBerry OS-Geräten, auf die keine IT-Richtlinien angewendet wurden

1. Klicken Sie in der Menüleiste auf **BlackBerry OS-Einstellungen**.
2. Erweitern Sie im Menü **Server und Komponenten** die Einträge **Topologie der BlackBerry-Lösung** > **BlackBerry Domain** > **Komponente: Anzeigen** > **Richtlinie**.
3. Klicken Sie auf die Instanz, die Sie ändern möchten.
4. Klicken Sie auf **Instanz bearbeiten**.
5. Klicken Sie in der Dropdown-Liste **Benutzer ohne angewendete IT-Richtlinie deaktivieren** auf **Wahr**.
6. Geben Sie im Feld **Zeitraum bis zur Deaktivierung des Benutzers (Stunden)** die Zeit (in Stunden) ein, nach der die PINs für BlackBerry OS-Geräte, auf die Sie keine IT-Richtlinie angewendet haben, unter BES12 deaktiviert werden.
7. Klicken Sie auf **Alles speichern**.

Wenn Sie fertig sind: Bevor Sie die BlackBerry OS- Geräte unter BES12 auf den Geräten in der Liste **Sicherheitsoptionen** reaktivieren, weisen Sie die Benutzer an, auf **Handheld löschen** oder **Sicherheitslöschung** zu klicken, um alle Daten auf den Geräten zu löschen.

Erstellen und Verwalten von BlackBerry OS IT-Richtlinien

Sie können vorkonfigurierte IT-Richtlinien zum Erstellen von benutzerdefinierten IT-Richtlinien für BlackBerry OS-Geräte (Version 5.0 bis 7.1) verwenden (um beispielsweise IT-Richtlinienregeln für verschiedene Benutzergruppen in Ihrer Organisation festzulegen). Wenn Sie planen, vorkonfigurierte BlackBerry OS-IT-Richtlinien einschließlich der Standard-IT-Richtlinie zu verwenden, sollten Sie diese überprüfen und bei Bedarf aktualisieren, um sicherzustellen, dass die Regeln die Sicherheitsstandards Ihrer Organisation erfüllen.

Erstellen einer BlackBerry OS-IT-Richtlinie

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf + neben I**T-Richtlinien** 5.0–7.1.
3. Geben Sie einen Namen und eine Beschreibung für die BlackBerry OS-IT-Richtlinie ein.
4. Klicken Sie auf **Hinzufügen**.
5. Führen Sie die folgenden Aktionen aus, um die BlackBerry OS-IT-Richtlinie zu konfigurieren:
   a. Klicken Sie auf **IT-Richtlinie bearbeiten**.
   b. Klicken Sie für jede Richtliniengruppe auf die Registerkarte, und konfigurieren Sie die entsprechenden Werte für die IT-Richtlinienregeln.
   c. Klicken Sie auf **Alles speichern**.

Wenn Sie fertig sind: Legen Sie die Rangordnung der BlackBerry OS-IT-Richtlinien fest.

Zuweisen eines Rangs zu BlackBerry OS-IT-Richtlinien

Wenn ein Benutzer Mitglied mehrerer Benutzergruppen mit verschiedenen BlackBerry OS-IT-Richtlinien ist, verwendet BES12 die Rangordnung, die Sie zum Lösen von in Konflikt stehenden IT-Richtlinien oder Einstellungen für IT-Richtlinienregeln festlegen.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Erweitern Sie im linken Fensterbereich **IT-Richtlinien** 5.0–7.1.
3. Klicken Sie auf **IT-Richtlinien einen Rang zuweisen**.
4. Mit den Pfeiltasten können Sie die BlackBerry OS-IT-Richtlinien in der Rangordnung nach oben oder unten verschieben.
5. Klicken Sie auf **Speichern**.

Verwandte Informationen

Zuweisen von BlackBerry OS-IT-Richtlinien und Auflösen von Konflikten zwischen IT-Richtlinien, auf Seite 146

Anzeigen einer BlackBerry OS-IT-Richtlinie

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Erweitern Sie im linken Fensterbereich **IT-Richtlinien** 5.0–7.1.
3. Klicken Sie auf den Namen der BlackBerry OS-IT-Richtlinie, die Sie anzeigen möchten.
4. Klicken Sie auf **Vollständige IT-Richtlinie anzeigen**.

Ändern einer BlackBerry OS-IT-Richtlinie

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Erweitern Sie im linken Fensterbereich **IT-Richtlinien** 5.0–7.1.
3. Klicken Sie auf den Namen der BlackBerry OS-IT-Richtlinie, die Sie ändern möchten.
4. Klicken Sie auf **IT-Richtlinie bearbeiten**.
5. Nehmen Sie die gewünschten Änderungen für jede Richtliniengruppe auf der entsprechenden Registerkarte vor.
6. Klicken Sie auf **Alles speichern**.

Wenn Sie fertig sind: Ändern Sie bei Bedarf die Rangordnung von BlackBerry OS-IT-Richtlinien.

Löschen einer BlackBerry OS-IT-Richtlinie

Sie können die standardmäßige BlackBerry OS-IT-Richtlinie nicht löschen. Wenn Sie eine benutzerdefinierte BlackBerry OS-IT-Richtlinie löschen, entfernt BES12 die IT-Richtlinie aus den Benutzern und deren verknüpften Geräten.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Erweitern Sie im linken Fensterbereich **IT-Richtlinien** 5.0–7.1.
3. Klicken Sie auf den Namen der BlackBerry OS-IT-Richtlinie, die Sie löschen möchten.
4. Klicken Sie auf .
5. Klicken Sie auf **Löschen**.

Verwandte Informationen

Zuweisen von BlackBerry OS-IT-Richtlinien und Auflösen von Konflikten zwischen IT-Richtlinien, auf Seite 146

Apps

Verteilen und verwalten Sie öffentliche, interne und gesicherte Apps auf Geräten.

Multiplatform

Verwalten von Apps auf Geräten

20

Sie können eine Bibliothek mit Apps erstellen, die Sie auf BlackBerry 10-, iOS-, Android- und Windows Phone-Geräten verwalten und überwachen möchten. Zum Verwalten von Apps können Sie der App-Liste die Apps hinzufügen und sie Benutzerkonten, Benutzergruppen oder Gerätegruppen zuweisen.

Schritte zum Verwalten von Apps

Um Apps zu verwalten, führen Sie die folgenden Aktionen aus:

Schritt	Aktion
1	Fügen Sie der App-Liste die Apps hinzu, die Sie verwalten möchten.
2	Erstellen Sie App-Gruppen zur gleichzeitigen Verwaltung mehrerer Apps bzw. zur Verwaltung von Apps auf Android for Work-Geräten.
3	Weisen Sie Apps oder App-Gruppen Benutzerkonten, Benutzergruppen oder Gerätegruppen hinzu, damit Benutzer sie installieren können.

Hinzufügen und Löschen von Apps aus der Liste der verfügbaren Apps

Die Liste der verfügbaren Apps enthält alle Apps, die Sie Benutzern, Benutzergruppen und Gerätegruppen zuweisen können. Mit einem Schlosssymbol versehene Apps sind gesicherte Apps, die mit iOS auf Android- und Secure Work Space-Geräten im geschäftlichen Bereich installiert werden können.

Hinzufügen von öffentlichen Apps zur App-Liste

Eine öffentliche App ist eine App, die über die BlackBerry World-Verkaufsplattform, den App Store-Online-Store, den Google Play-Store oder den Windows Phone Store erhältlich ist.

Hinzufügen einer BlackBerry-App zur App-Liste

1. Klicken Sie in der Menüleiste auf **Apps**.
2. Klicken Sie auf .
3. Klicken Sie auf **BlackBerry World**.

4. Suchen Sie im Suchfeld nach der App, die Sie hinzufügen möchten. Sie können nach App-Name, Anbieter oder BlackBerry World-URL suchen.
5. Wählen Sie in der Dropdown-Liste das Land des Stores aus, in dem Sie suchen möchten.
6. Klicken Sie auf **Suchen**.
7. Klicken Sie in den Suchergebnissen auf **Hinzufügen**, um eine App hinzuzufügen.
8. Klicken Sie im App-Informationsbildschirm auf **Hinzufügen**.

Hinzufügen einer iOS-App zur App-Liste

Bevor Sie beginnen: Wenn die Enterprise-Konnektivität aktiviert ist, müssen bei einigen sicheren Apps, die im App Store verfügbar sind, bestimmte Ports in BES12 geöffnet werden. Informationen erhalten Sie vom App-Anbieter.

1. Klicken Sie in der Menüleiste auf **Apps**.
2. Klicken Sie auf .
3. Klicken Sie auf **App Store**.
4. Suchen Sie im Suchfeld nach der App, die Sie hinzufügen möchten. Sie können nach App-Name, Anbieter oder App Store-URL suchen.
5. Wählen Sie in der Dropdown-Liste das Land des Stores aus, in dem Sie suchen möchten.
6. Klicken Sie auf **Suchen**.
7. Klicken Sie in den Suchergebnissen auf **Hinzufügen**, um eine App hinzuzufügen.
8. Wählen Sie in der Dropdown-Liste **Unterstützter Formfaktor des Geräts** die Formfaktoren aus, auf denen die App installiert werden kann. Beispielsweise können Sie verhindern, dass die App in der App „Geschäftliche Apps“ für iPad verfügbar ist.
9. Wenn Sie die App vom Gerät entfernen möchten, wenn das Gerät von BES12 entfernt wird, wählen Sie **Die App vom Gerät entfernen, wenn das Gerät von BES12 entfernt wird**. Diese Option gilt nur für Apps, deren Verfügbarkeit auf „Erforderlich“ und deren Standardinstallation für erforderliche Apps auf „Einmal auffordern“ festgelegt ist.
10. Wenn Apps auf iOS-Geräten nicht in den iCloud-Onlinedienst gesichert werden sollen, wählen Sie **iCloud-Sicherung für die App deaktivieren**. Diese Option gilt nur für Apps, deren Verfügbarkeit auf „Erforderlich“ festgelegt ist. Die Verfügbarkeit der App wird festgelegt, wenn Sie die App einem Benutzer oder einer Gruppe zuweisen.
11. Führen Sie in der Dropdown-Liste **Standardinstallation für erforderliche Apps** eine der folgenden Aktionen aus:
    - Wenn Benutzer eine Aufforderung zur Installation der App auf ihren iOS-Geräten erhalten sollen, wählen Sie **Einmal auffordern** aus. Wenn der Benutzer die Aufforderung schließt, kann er die App später über den Bildschirm „Geschäftliche Apps“ im BES12 Client oder über das Symbol „Geschäftliche Apps“ auf dem Gerät installieren.
    - Wenn Benutzer keine Aufforderung erhalten sollen, wählen Sie **Keine Eingabeaufforderung**.

    Die Standardinstallationsmethode gilt nur für Apps, deren Verfügbarkeit auf „Erforderlich“ festgelegt ist. Die Verfügbarkeit der App wird festgelegt, wenn Sie die App einem Benutzer oder einer Gruppe zuweisen.

12. Klicken Sie auf **Hinzufügen**.

Hinzufügen einer Android-App zur App-Liste

Hinzufügen von Apps (ausschließlich) zur Liste der verfügbaren Apps Filme, Musik und Medien aus dem Zeitungskiosk können nicht an Geräte gesendet werden. Wenn Sie einem Benutzer Medien zuweisen und die Verfügbarkeit der Medien auf „Erforderlich“ festlegen, ist das Gerät an die Erzwingungsaktion gebunden, die im Kompatibilitätsprofil festgelegt und dem Gerät zugewiesen wurde.

Bevor Sie beginnen: Wenn die Enterprise-Konnektivität aktiviert ist, müssen bei einigen sicheren Apps, die in Google Play verfügbar sind, bestimmte Ports in BES12 geöffnet werden. Informationen erhalten Sie vom App-Anbieter.

1. Klicken Sie in der Menüleiste auf **Apps**.
2. Klicken Sie auf .
3. Klicken Sie auf **Google Play**.
4. Klicken Sie auf **Google Play öffnen**, und suchen Sie nach der App, die Sie hinzufügen möchten. Sie können dann die Informationen aus Google Play in den folgenden Schritten kopieren und einfügen sowie Symbole und Screenshots herunterladen.
5. Geben Sie im Feld **App-Name** den Namen der App ein.
6. Geben Sie im Feld **App-Beschreibung** eine Beschreibung für die App ein.
7. Geben Sie im Feld **Anbieter** den Namen des Anbieters der App ein.
8. Klicken Sie im Feld **App-Symbol** auf **Durchsuchen**. Suchen Sie ein Symbol für die App, und wählen Sie es aus. Folgende Formate werden unterstützt: .png, .jpg, .jpeg oder .gif. Verwenden Sie nicht Google Chrome, um das Symbol herunterzuladen, da ansonsten ein nicht kompatibles .webp-Bild heruntergeladen wird.
9. Geben Sie im Feld **App-Webadresse von Google Play** die Webadresse der App in Google Play ein.
10. Um Screenshots der App hinzuzufügen, klicken Sie auf **Hinzufügen**, und navigieren Sie zu den Screenshots. Folgende Bilddateitypen werden unterstützt: .jpg, .jpeg, .png oder .gif.
11. Führen Sie in der Dropdown-Liste **Senden an** eine der folgenden Aktionen aus:
    - Wenn die App auf alle Android-Geräte gesendet werden soll, wählen Sie **Alle Android-Geräte**.
    - Wenn die App nur auf Android-Geräte mit Samsung KNOX Workspace gesendet werden soll, wählen Sie **Nur KNOX Workspace-Geräte**.
12. Klicken Sie auf **Hinzufügen**.

Hinzufügen einer Android-App zur App-Liste bei Verbindung von BES12 mit einer Google-Domäne

Wenn Sie eine Android for Work-Verbindung konfiguriert haben, können Sie Apps auf allen Android-Geräten, einschließlich solcher mit Android for Work verwalten. Weitere Informationen über das Konfigurieren von BES12 zur Unterstützung von Android for Work finden Sie in der Dokumentation zur Konfiguration unter help.blackberry.com/detectLang/bes12/.

1. Klicken Sie in der Menüleiste auf **Apps**.
2. Klicken Sie auf .
3. Klicken Sie auf **Google Play**.
4. Geben Sie im Feld **App-URL von Google Play** die Webadresse der App in Google Play ein.
5. Klicken Sie auf **Suchen**.
6. Klicken Sie in den Suchergebnissen auf **Hinzufügen**, um eine App hinzuzufügen.
7. Klicken Sie auf **Annehmen**, um App-Berechtigungen im Namen von Benutzern anzunehmen. Sie müssen App-Berechtigungen im Namen von Benutzern annehmen, damit erforderliche Apps automatisch auf Android for Work-Geräten installiert werden können. Wenn Sie die App-Berechtigungen nicht im Namen der Benutzer annehmen, kann die App nicht in BES12 verwaltet werden.
8. Klicken Sie auf **Weiter**.
9. Um Screenshots der App hinzuzufügen, klicken Sie auf **Hinzufügen**, und navigieren Sie zu den Screenshots. Folgende Bilddateitypen werden unterstützt: .jpg, .jpeg, .png oder .gif.
10. Führen Sie in der Dropdown-Liste **Senden an** eine der folgenden Aktionen aus:
    - Wenn die App auf alle Android-Geräte gesendet werden soll, wählen Sie **Alle Android-Geräte**.
    - Wenn die App nur auf Android-Geräte mit Samsung KNOX Workspace gesendet werden soll, wählen Sie **Nur KNOX Workspace-Geräte**.
11. Eine App-Konfigurationstabelle wird nur angezeigt, wenn es für die App Konfigurationseinstellungen gibt. Klicken Sie auf + in der App-Konfigurationstabelle, um eine App-Konfiguration hinzuzufügen.
12. Falls erforderlich, geben Sie einen Namen für die App-Konfiguration und die Konfigurationseinstellungen an. Klicken Sie auf **Speichern**.
13. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Wenn Sie eine App auf einem Android for Work-Gerät installieren möchten, müssen Sie die App einer App-Gruppe hinzufügen, die für Android for Work aktiviert wurde, und die App-Gruppe einem Benutzer oder einer Benutzergruppe zuweisen.

Hinzufügen einer Windows Phone-App zur App-Liste

1. Klicken Sie in der Menüleiste auf **Apps**.
2. Klicken Sie auf .
3. Klicken Sie auf **Windows Phone Store**.
4. Klicken Sie auf **Windows Phone Store öffnen**, und suchen Sie nach der App, die Sie hinzufügen möchten. Sie können dann die Informationen aus Windows Phone Store in den folgenden Schritten kopieren und einfügen sowie Symbole und Screenshots herunterladen.
5. Geben Sie im Feld **App-Name** den Namen der App ein.

6. Geben Sie im Feld **App-Beschreibung** eine Beschreibung für die App ein.
7. Geben Sie im Feld **Anbieter** den Namen des Anbieters der App ein.
8. Klicken Sie im Feld **App-Symbol** auf **Durchsuchen**. Suchen Sie ein Symbol für die App, und wählen Sie es aus. Folgende Formate werden unterstützt: .png, .jpg, .jpeg oder .gif.
9. Geben Sie im Feld **App-Webadresse im Windows Phone Store** die Webadresse der App in Windows Phone Store ein.
10. Um Screenshots der App hinzuzufügen, klicken Sie auf **Hinzufügen**, und navigieren Sie zu den Screenshots. Folgende Bilddateitypen werden unterstützt: .jpg, .jpeg, .png oder .gif.
11. Klicken Sie auf **Hinzufügen**.

Hinzufügen von internen Apps zur App-Liste

Interne Apps umfassen proprietäre Apps, die von Ihrer Organisation entwickelt wurden, oder Apps, die Ihrer Organisation zur exklusiven Verwendung bereitgestellt wurden. Interne Apps werden nicht über öffentliche App-Verkaufsplattformen hinzugefügt.

BlackBerry-Apps müssen als BAR-Dateien, iOS-Apps als IPA-Dateien, Android-Apps als APK-Dateien und Windows Phone-Apps als XAP- oder APPX-Dateien vorliegen. Interne Apps werden auf der Registerkarte „Geschäftliche Apps“ in BlackBerry World for Work auf BlackBerry 10-Geräten und in der Liste „Zugewiesene geschäftliche Apps“ im BES12 Client auf iOS-, Android- und Windows Phone-Geräten angezeigt. Interne Apps müssen zudem signiert sein und dürfen nicht verändert werden.

BlackBerry 10-, Windows Phone- und Android-Apps auf Geräten mit Samsung KNOX mit der Verfügbarkeitseinstellung „Erforderlich“ werden automatisch auf allen entsprechenden Geräten installiert, denen sie zugewiesen sind.

Schritte zum Hinzufügen von internen Apps zur App-Liste

Um interne Apps hinzuzufügen, führen Sie die folgenden Aktionen aus:

Schritt	Aktion
1	Geben Sie den freigegebenen Netzwerkpfad zur Speicherung interner Apps an.
2	Wenn Sie Windows Phone-Apps hinzufügen, laden Sie ein AET hoch.
3	Fügen Sie der App-Liste eine interne App hinzu.

Angeben des freigegebenen Netzwerkpfads zur Speicherung interner Apps

Bevor Sie interne Apps der Liste verfügbarer Apps hinzufügen können, müssen Sie einen freigegebenen Netzwerkpfad zur Speicherung der App-Quelldateien angeben. Um sicherzustellen, dass die internen Apps verfügbar bleiben, sollte dieser Netzwerkpfad über eine Hochverfügbarkeitslösung verfügen und regelmäßig gesichert werden. Erstellen Sie den Ordner außerdem nicht im BES12-Installationsordner, da er sonst gelöscht wird, wenn Sie ein Upgrade von BES12 durchführen.

Bevor Sie beginnen:

- Erstellen Sie einen freigegebenen Netzwerkordner, um die Quelldateien für interne Apps in dem Netzwerk zu speichern, das BES12 hostet.
- Überprüfen Sie, ob das Dienstkonto des Computers, der BES12 hostet, über Lese- und Schreibzugriff auf den freigegebenen Netzwerkordner verfügt.

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Erweitern Sie im linken Fensterbereich die Option **App-Verwaltung**.
3. Klicken Sie auf **Speicher für interne Apps**.
4. Geben Sie im Feld **Netzwerkpfad** den Pfad des freigegebenen Netzwerkordners im folgenden Format ein:

   \\<*computer_name*>\<*shared_network_folder*>

   Der freigegebene Netzwerkpfad muss im UNC-Format eingegeben werden (Beispiel: \\ComputerName\Applications\InternalApps).
5. Klicken Sie auf **Speichern**.

Hochladen eines Anwendungsinstallations-Tokens (AET)

Bevor Benutzer interne Apps auf Windows Phone-Geräten installieren können, müssen sie ein AET hochladen. Die Apps, die Benutzer installieren sollen, müssen das gleiche Zertifikat wie der hochgeladene AET nutzen. Weitere Informationen zur Generierung eines Anwendungsinstallations-Tokens finden Sie auf msdn.microsoft.com unter *How to generate an application enrollment token for Windows Phone* (Generieren eines Anwendungsinstallations-Tokens für Windows Phone). Sie benötigen außerdem ein AET, wenn Sie interne oder öffentliche Windows-Apps in Kompatibilitätsprofilen überwachen möchten.

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Erweitern Sie im linken Fensterbereich die Option **App-Verwaltung**.
3. Klicken Sie auf **Windows Phone Apps**.
4. Klicken Sie auf **Durchsuchen**, und navigieren Sie zu dem AET, den Sie hochladen möchten.
5. Klicken Sie auf **Speichern**.

Hinzufügen einer internen App zur Liste der verfügbaren Apps

Bevor Sie beginnen:

- Geben Sie den freigegebenen Netzwerkpfad zur Speicherung interner Apps an.
- Wenn Sie Windows Phone-Apps hinzufügen, laden Sie ein AET hoch.

1. Klicken Sie in der Menüleiste auf **Apps**.
2. Klicken Sie auf .
3. Klicken Sie auf **Interne Apps**.
4. Klicken Sie auf **Durchsuchen**, und navigieren Sie zu der App, die Sie hinzufügen oder aktualisieren möchten.

5. Klicken Sie auf **Öffnen**.
6. Klicken Sie auf **Hinzufügen**.
7. Geben Sie optional einen Anbieternamen und eine App-Beschreibung ein.
8. Um Screenshots der App hinzuzufügen, klicken Sie auf **Hinzufügen**, und navigieren Sie zu den Screenshots. Folgende Bilddateitypen werden unterstützt: .jpg, .jpeg, .png oder .gif.
9. Führen Sie beim Hinzufügen einer iOS-App eine der folgenden Aktionen aus:
   a. Wählen Sie in der Dropdown-Liste **Unterstützter Formfaktor des Geräts** die Formfaktoren aus, auf denen die App installiert werden kann. Beispielsweise können Sie verhindern, dass die App in der App „Geschäftliche Apps“ für iPad verfügbar ist.
   b. Wenn Sie die App vom Gerät entfernen möchten, wenn das Gerät von BES12 entfernt wird, wählen Sie **Die App vom Gerät entfernen, wenn das Gerät von BES12 entfernt wird**. Diese Option gilt nur für Apps, deren Verfügbarkeit auf „Erforderlich“ und deren Standardinstallation für erforderliche Apps auf „Einmal auffordern“ festgelegt ist.
   c. Wenn Apps auf iOS-Geräten nicht in den iCloud-Onlinedienst gesichert werden sollen, wählen Sie **iCloud-Sicherung für die App deaktivieren**. Diese Option gilt nur für Apps, deren Verfügbarkeit auf „Erforderlich“ festgelegt ist. Die Verfügbarkeit der App wird festgelegt, wenn Sie die App einem Benutzer oder einer Gruppe zuweisen.
   d. Wenn Benutzer eine Aufforderung zur Installation der App auf ihren Geräten mit iOS erhalten sollen, wählen Sie in der Dropdown-Liste **Standardinstallation für erforderliche Apps** die Option **Einmal auffordern**. Wenn der Benutzer die Aufforderung schließt, kann er die App später über „Geschäftliche Apps“ im BES12 Client oder über das Symbol „Geschäftliche Apps“ auf dem Gerät installieren.
10. Wenn Sie eine Android-App hinzufügen, führen Sie in der Dropdown-Liste **Senden an** eine der folgenden Aktionen aus:
    - Wenn die App auf alle Android-Geräte gesendet werden soll, wählen Sie **Alle Android-Geräte**.
    - Wenn die App nur auf Android-Geräte mit Samsung KNOX Workspace gesendet werden soll, wählen Sie **Nur KNOX Workspace-Geräte**.
11. Klicken Sie auf **Hinzufügen**.

Hinzufügen von gesicherten Apps zur App-Liste

Gesicherte Apps werden speziell zur Ausführung im geschäftlichen Bereich von iOS- und Android-Geräten mit Secure Work Space entwickelt. Gesicherte Apps bieten die gleiche Sicherheitsstufe wie Apps, die im geschäftlichen Bereich auf BlackBerry 10-Geräten installiert sind. iOS-Apps müssen als IPA-Dateien und Android-Apps als APK-Dateien vorliegen. Gesicherte Apps müssen gewrappt und signiert sein.

Gesicherte Apps werden in der App-Liste mit einem Schlosssymbol angezeigt.

Schritte zum Hinzufügen von gesicherten Apps zur App-Liste

Um gesicherte Apps zu verwalten, führen Sie die folgenden Aktionen aus:

Schritt	Aktion
1	Geben Sie an, welche benutzerdefinierten Apps Sie für iOS- oder Android-Geräte sichern möchten.
2	Sichern Sie die App über die Verwaltungskonsole für die Verwendung im geschäftlichen Bereich.
3	Nachdem die App gesichert wurde, laden Sie die gesicherte Datei aus der Verwaltungskonsole herunter.
4	Lassen Sie die App vom Entwickler erneut signieren.
5	Nachdem Sie die erneut signierte App vom Entwickler erhalten haben, fügen Sie die App der Liste der verfügbaren Apps in der Verwaltungskonsole hinzu.

Sichern einer App

Verwenden Sie die Verwaltungskonsole zum Sichern einer App, damit sie im geschäftlichen Bereich von iOS- und Android-Geräten installiert werden kann.

Bevor Sie beginnen:

- Beziehen Sie die App-Binärdatei (.apk oder .ipa) vom Entwickler. Die App darf nicht mehr als 50 MB groß sein.

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Erweitern Sie im linken Fensterbereich die Option **Externe Integration**.
3. Klicken Sie auf **Secure Work Space**.
4. Navigieren Sie im Abschnitt zum **Sichern einer App** zur Anwendungsdatei (.apk oder .ipa), und klicken Sie auf **Upload**.
5. Überprüfen Sie den Status der App. Der Vorgang kann einige Minuten bis mehrere Stunden dauern.
6. Wenn der Status angibt, dass die **Sicherung abgeschlossen** ist, klicken Sie auf **Download**, um die gesicherte App auf Ihren lokalen Computer herunterzuladen.

Wenn Sie fertig sind:

- Lassen Sie die gesicherte App vom Entwickler erneut signieren.
- Fügen Sie die App zur Liste der verfügbaren Apps hinzu.

Erneutes Signieren einer App

Nachdem Sie eine iOS- oder Android-App gesichert haben, muss diese vom Entwickler erneut signiert werden. Die gesicherte und erneut signierte App wird zur Verteilung an den Administrator zurückgegeben.

Wenn eine gesicherte App für iOS-Geräte auf bestimmte iOS-Ressourcen zugreifen oder bestimmte Vorgänge (z. B. Push-Benachrichtigungen) durchführen muss, hat der App-Entwickler eine bestimmte Datei mit Berechtigungseinstellungen zu erstellen.

Weitere Informationen finden Sie unter developer.blackberry.com/devzone im Abschnitt *Erneutes Signieren einer App*.

Löschen einer App aus der App-Liste

Wenn Sie eine App aus der App-Liste löschen, wird die derzeitige Zuweisung der App zu allen Benutzern oder Gruppen aufgehoben, und die App wird nicht mehr im Katalog der geschäftlichen Apps auf dem Gerät angezeigt.

1. Klicken Sie in der Menüleiste auf **Apps**.
2. Aktivieren Sie die Kontrollkästchen neben den Apps, die Sie aus der App-Liste löschen möchten.
3. Klicken Sie auf 🗑.
4. Klicken Sie auf **Löschen**.

App-Verhalten auf Android-Geräten

Bei Geräten, die mit „MDM-Steuerelemente“, „Geschäftlich und persönlich – vollständige Kontrolle (Secure Work Space)“ und „Geschäftlich und persönlich – Benutzer-Datenschutz (Secure Work Space)“ aktiviert wurden, gilt Folgendes:

App-Typ	Verhalten bei App-Zuweisung	Verhalten bei Aufhebung der App-Zuweisung	Verhalten bei Entfernen des Geräts aus BES12
Öffentliche Apps mit Verfügbarkeitseinstellung „Erforderlich“	• Der Benutzer wird aufgefordert, die Apps zu installieren. • Die Apps werden in der Liste „Zugewiesene geschäftliche Apps“ im BES12 Client angezeigt. • Sie können mit einem Kompatibilitätsprofil die Aktionen definieren, die eintreten, wenn erforderliche Apps nicht installiert werden.	• Der Benutzer wird aufgefordert, die Apps zu entfernen. • Die Apps werden nicht mehr in der Liste „Zugewiesene geschäftliche Apps“ im BES12 Client angezeigt.	• Der Benutzer wird aufgefordert, die Apps zu entfernen.
Öffentliche Apps mit Verfügbarkeitseinstellung „Optional“	• Der Benutzer kann wählen, ob er die Apps installieren möchte.	• Der Benutzer wird aufgefordert, die Apps zu entfernen.	• Der Benutzer wird aufgefordert, die Apps zu entfernen.

App-Typ	Verhalten bei App-Zuweisung	Verhalten bei Aufhebung der App-Zuweisung	Verhalten bei Entfernen des Geräts aus BES12
	• Die Apps werden in der Liste „Zugewiesene geschäftliche Apps“ im BES12 Client angezeigt.	• Die Apps werden nicht mehr in der Liste „Zugewiesene geschäftliche Apps“ im BES12 Client angezeigt.	
Interne Apps mit Verfügbarkeitseinstellung „Erforderlich“	• Der Benutzer wird aufgefordert, die Apps zu installieren. • Die Apps werden in der Liste „Zugewiesene geschäftliche Apps“ im BES12 Client angezeigt. • Sie können mit einem Kompatibilitätsprofil die Aktionen definieren, die eintreten, wenn erforderliche Apps nicht installiert werden.	• Der Benutzer wird aufgefordert, die Apps zu entfernen. • Die Apps werden nicht mehr in der Liste „Zugewiesene geschäftliche Apps“ im BES12 Client angezeigt.	• Der Benutzer wird aufgefordert, die Apps zu entfernen.
Interne Apps mit Verfügbarkeitseinstellung „Optional“	• Der Benutzer kann wählen, ob er die Apps installieren möchte. • Die Apps werden in der Liste „Zugewiesene geschäftliche Apps“ im BES12 Client angezeigt.	• Der Benutzer wird aufgefordert, die Apps zu entfernen. • Die Apps werden nicht mehr in der Liste „Zugewiesene geschäftliche Apps“ im BES12 Client angezeigt.	• Der Benutzer wird aufgefordert, die Apps zu entfernen.

Bei Samsung KNOX-Geräten, die mit „MDM-Steuerelemente“ aktiviert wurden, gilt Folgendes:

App-Typ	Verhalten bei App-Zuweisung	Verhalten bei Aufhebung der App-Zuweisung	Verhalten bei Entfernen des Geräts aus BES12
Öffentliche Apps mit Verfügbarkeitseinstellung „Erforderlich“	• Der Benutzer wird aufgefordert, die Apps zu installieren.	• Der Benutzer wird aufgefordert, die Apps zu deinstallieren.	• Der Benutzer wird aufgefordert, zugewiesene

App-Typ	Verhalten bei App-Zuweisung	Verhalten bei Aufhebung der App-Zuweisung	Verhalten bei Entfernen des Geräts aus BES12
	• Zugewiesene Apps werden im BES12 Client angezeigt. Wenn der Benutzer auf die Schaltfläche zum Installieren klickt, öffnet sich Google Play, und die App wird von dort installiert. • Sie können mit einem Kompatibilitätsprofil die Aktionen definieren, die eintreten, wenn erforderliche Apps nicht installiert werden.		geschäftliche Apps zu deinstallieren.
Öffentliche Apps mit Verfügbarkeitseinstellung „Optional“	• Der Benutzer kann wählen, ob er die Apps installieren möchte. • Zugewiesene Apps werden im BES12 Client angezeigt. Wenn der Benutzer auf die Schaltfläche zum Installieren klickt, öffnet sich Google Play, und Apps werden von dort installiert.	• Der Benutzer wird aufgefordert, die Apps zu deinstallieren.	• Der Benutzer wird aufgefordert, zugewiesene geschäftliche Apps zu deinstallieren.
Interne Apps mit Verfügbarkeitseinstellung „Erforderlich“	• Die Apps werden automatisch auf Geräten installiert. Der Benutzer kann die Apps nicht deinstallieren. • Zugewiesene Apps werden vom BES12 Client installiert.	• Die Apps werden automatisch vom Gerät entfernt.	• Die Apps werden automatisch vom Gerät entfernt.

App-Typ	Verhalten bei App-Zuweisung	Verhalten bei Aufhebung der App-Zuweisung	Verhalten bei Entfernen des Geräts aus BES12
Interne Apps mit Verfügbarkeitseinstellung „Optional“	• Der Benutzer kann wählen, ob er die Apps installieren möchte. • Zugewiesene Apps werden vom BES12 Client installiert.	• Die Apps werden automatisch vom Gerät entfernt.	• Die Apps werden automatisch vom Gerät entfernt.

Bei Samsung KNOX-Geräten, die nur mit geschäftlichem Bereich aktiviert wurden (Samsung KNOX), gilt Folgendes:

App-Typ	Verhalten bei App-Zuweisung	Verhalten bei Aufhebung der App-Zuweisung	Verhalten bei Entfernen des Geräts aus BES12
Öffentliche Apps mit Verfügbarkeitseinstellung „Erforderlich“	• Alle öffentlichen Apps sind standardmäßig im geschäftlichen Bereich eingeschränkt. • Zugewiesene Apps werden im BES12 Client angezeigt, müssen jedoch aus Google Play installiert werden. • Google Play muss in der IT-Richtlinie aktiviert sein, die dem Benutzer zugewiesen ist. • Sie können mit einem Kompatibilitätsprofil die Aktionen definieren, die eintreten, wenn eine erforderliche App nicht installiert wird.	• Die Apps werden von dem Gerät entfernt und können nicht mehr von Google Play installiert werden.	• Der geschäftliche Bereich und alle geschäftlichen Apps werden automatisch entfernt. • Apps sind nicht mehr automatisch in Google Play eingeschränkt.
Öffentliche Apps mit Verfügbarkeitseinstellung „Optional“	• Alle Apps sind standardmäßig im geschäftlichen Bereich eingeschränkt. • Zugewiesene Apps werden im BES12 Client	• Die Apps werden von dem Gerät entfernt und können nicht mehr von Google Play installiert werden.	• Der geschäftliche Bereich und alle geschäftlichen Apps werden automatisch entfernt.

App-Typ	Verhalten bei App-Zuweisung	Verhalten bei Aufhebung der App-Zuweisung	Verhalten bei Entfernen des Geräts aus BES12
	angezeigt, müssen jedoch aus Google Play installiert werden. • Google Play muss in der IT-Richtlinie aktiviert sein, die dem Benutzer zugewiesen ist.		• Apps sind nicht mehr automatisch in Google Play eingeschränkt.
Interne Apps mit Verfügbarkeitseinstellung „Erforderlich“	• Die Apps werden automatisch auf Geräten installiert. Der Benutzer kann die Apps nicht deinstallieren.	• Die Apps werden automatisch vom Gerät entfernt.	• Der geschäftliche Bereich und alle geschäftlichen Apps werden automatisch entfernt.
Interne Apps mit Verfügbarkeitseinstellung „Optional“	• Der Benutzer kann wählen, ob er die Apps installieren möchte. • Zugewiesene Apps werden vom BES12 Client installiert.	• Die Apps werden automatisch vom Gerät entfernt.	• Der geschäftliche Bereich und alle geschäftlichen Apps werden automatisch entfernt.

Bei Geräten, die mit „Geschäftlich und persönlich – vollständige Kontrolle (Samsung KNOX)“ aktiviert wurden, gilt Folgendes:

App-Typ	Verhalten bei App-Zuweisung	Verhalten bei Aufhebung der App-Zuweisung	Verhalten bei Entfernen des Geräts aus BES12
Öffentliche Apps mit Verfügbarkeitseinstellung „Erforderlich“	• Alle öffentlichen Apps sind standardmäßig im geschäftlichen Bereich eingeschränkt. • Der Benutzer wird aufgefordert, die Apps zu installieren. • Zugewiesene Apps werden im BES12 Client angezeigt. Wenn der Benutzer auf die Schaltfläche zum	• Die Apps verbleiben im persönlichen Bereich, werden jedoch aus dem geschäftlichen Bereich entfernt.	• Der geschäftliche Bereich wird entfernt, und die Apps verbleiben im persönlichen Bereich.

App-Typ	Verhalten bei App-Zuweisung	Verhalten bei Aufhebung der App-Zuweisung	Verhalten bei Entfernen des Geräts aus BES12
	Installieren klickt, öffnet sich Google Play, und die App wird von dort installiert. • Sie können mit einem Kompatibilitätsprofil die Aktionen definieren, die eintreten, wenn eine erforderliche App nicht installiert wird.		
Öffentliche Apps mit Verfügbarkeitseinstellung „Optional“	• Alle Apps sind standardmäßig im geschäftlichen Bereich eingeschränkt. • Zugewiesene Apps werden im BES12 Client angezeigt, müssen jedoch aus Google Play installiert werden. • Google Play muss in der IT-Richtlinie aktiviert sein, die dem Benutzer zugewiesen ist.	• Die Apps verbleiben im persönlichen Bereich, werden jedoch aus dem geschäftlichen Bereich entfernt.	• Der geschäftliche Bereich wird entfernt, und die Apps verbleiben im persönlichen Bereich.
Interne Apps mit Verfügbarkeitseinstellung „Erforderlich“	• Die Apps werden automatisch auf Geräten installiert. Der Benutzer kann die Apps nicht deinstallieren.	• Die Apps werden automatisch vom Gerät entfernt.	• Der geschäftliche Bereich wird entfernt, und die Apps verbleiben im persönlichen Bereich.
Interne Apps mit Verfügbarkeitseinstellung „Optional“	• Der Benutzer kann wählen, ob er die Apps installieren möchte. • Zugewiesene Apps werden vom BES12 Client installiert.	• Die Apps werden automatisch vom Gerät entfernt.	• Der geschäftliche Bereich wird entfernt, und die Apps verbleiben im persönlichen Bereich.

Bei Geräten, die mit „Geschäftlich und persönlich – Benutzer-Datenschutz (Android for Work)“ aktiviert wurden, gilt Folgendes:

App-Typ	Verhalten bei App-Zuweisung	Verhalten bei Aufhebung der App-Zuweisung	Verhalten bei Entfernen des Geräts aus BES12
Öffentliche Apps mit Verfügbarkeitseinstellung „Erforderlich“	• Die Apps werden automatisch installiert. • Zugewiesene Apps werden vom BES12 Client installiert.	• Die Apps werden automatisch vom Gerät entfernt.	• Das Geschäftsprofil und zugewiesene geschäftliche Apps werden von dem Gerät entfernt.
Öffentliche Apps mit Verfügbarkeitseinstellung „Optional“	• Der Benutzer kann wählen, ob er die Apps installieren möchte. • Die Apps werden in Google Play for Work angezeigt.	• Die Apps werden automatisch vom Gerät entfernt.	• Das Geschäftsprofil und zugewiesene geschäftliche Apps werden von dem Gerät entfernt.
Interne Apps mit Verfügbarkeitseinstellung „Erforderlich“	• Nicht unterstützt.	• Nicht unterstützt.	• Nicht unterstützt.
Interne Apps mit Verfügbarkeitseinstellung „Optional“	• Nicht unterstützt.	• Nicht unterstützt.	• Nicht unterstützt.

App-Verhalten auf iOS-Geräten

Bei Geräten, die mit „MDM-Steuerelemente“, „Geschäftlich und persönlich – vollständige Kontrolle (Secure Work Space)“ und „Geschäftlich und persönlich – Benutzer-Datenschutz (Secure Work Space)“ aktiviert wurden, gilt Folgendes:

App-Typ	Verhalten bei App-Zuweisung	Verhalten bei Aufhebung der App-Zuweisung	Verhalten bei Entfernen des Geräts aus BES12
Öffentliche Apps mit Verfügbarkeitseinstellung „Erforderlich“	• Je nach Apps-Einstellungen wird der Benutzer ggf. zur Installation der Apps aufgefordert. • Die Apps werden in der App „Geschäftliche Apps“ oder im BES12	• Die Apps werden automatisch vom Gerät entfernt. • Die Apps werden nicht mehr in der App „Geschäftliche Apps“ oder im BES12 Client auf Geräten angezeigt,	• Bei Geräten mit Secure Work Space werden der geschäftliche Bereich und alle geschäftlichen Apps automatisch entfernt. • Bei mit MDM-Steuerelemente

App-Typ	Verhalten bei App-Zuweisung	Verhalten bei Aufhebung der App-Zuweisung	Verhalten bei Entfernen des Geräts aus BES12
	Client auf Geräten angezeigt, die mit „Privatsphäre des Benutzers“ aktiviert wurden. • Sie können mit einem Kompatibilitätsprofil die Aktionen definieren, die eintreten, wenn erforderliche Apps nicht installiert werden.	die mit „Privatsphäre des Benutzers“ aktiviert wurden.	aktivierten Geräten werden alle Apps aus dem geschäftlichen Bereich automatisch entfernt.
Öffentliche Apps mit Verfügbarkeitseinstellung „Optional“	• Der Benutzer kann wählen, ob er die Apps installieren möchte. • Die Apps werden in der App „Geschäftliche Apps“ oder im BES12 Client auf Geräten angezeigt, die mit „Privatsphäre des Benutzers“ aktiviert wurden.	• Die Apps werden automatisch vom Gerät entfernt. • Die Apps werden nicht mehr in der App „Geschäftliche Apps“ oder im BES12 Client auf Geräten angezeigt, die mit „Privatsphäre des Benutzers“ aktiviert wurden.	• Bei Geräten mit Secure Work Space werden der geschäftliche Bereich und alle geschäftlichen Apps automatisch entfernt. • Bei mit MDM-Steuerelemente aktivierten Geräten werden alle Apps aus dem geschäftlichen Bereich automatisch entfernt.
Interne Apps mit Verfügbarkeitseinstellung „Erforderlich“	• Je nach App-Einstellungen wird der Benutzer ggf. zur Installation der App aufgefordert. • Die Apps werden in der App „Geschäftliche Apps“ oder im BES12 Client auf Geräten angezeigt, die mit „Privatsphäre des Benutzers“ aktiviert wurden.	• Die Apps werden automatisch vom Gerät entfernt. • Die Apps werden nicht mehr in der App „Geschäftliche Apps“ oder im BES12 Client auf Geräten angezeigt, die mit „Privatsphäre des Benutzers“ aktiviert wurden.	• Bei Geräten mit Secure Work Space werden der geschäftliche Bereich und alle geschäftlichen Apps automatisch entfernt. • Bei mit MDM-Steuerelemente aktivierten Geräten werden alle Apps aus dem geschäftlichen Bereich automatisch entfernt.

App-Typ	Verhalten bei App-Zuweisung	Verhalten bei Aufhebung der App-Zuweisung	Verhalten bei Entfernen des Geräts aus BES12
	• Sie können mit einem Kompatibilitätsprofil die Aktionen definieren, die eintreten, wenn erforderliche Apps nicht installiert werden.		
Interne Apps mit Verfügbarkeitseinstellung „Optional“	• Der Benutzer kann wählen, ob er die Apps installieren möchte. • Die Apps werden in der App „Geschäftliche Apps“ oder im BES12 Client auf Geräten angezeigt, die mit „Privatsphäre des Benutzers“ aktiviert wurden.	• Die Apps werden automatisch vom Gerät entfernt. • Die Apps werden nicht mehr in der App „Geschäftliche Apps“ oder im BES12 Client auf Geräten angezeigt, die mit „Privatsphäre des Benutzers“ aktiviert wurden.	• Bei Geräten mit Secure Work Space werden der geschäftliche Bereich und alle geschäftlichen Apps automatisch entfernt. • Bei mit MDM-Steuerelemente aktivierten Geräten werden alle Apps aus dem geschäftlichen Bereich automatisch entfernt.

App-Verhalten auf BlackBerry-Geräten

Bei BlackBerry-Geräten, die mit „Geschäftlich und persönlich – Unternehmen (Nur geschäftlicher Bereich)“ oder Geschäftlich und persönlich – Reguliert aktiviert wurden, gilt Folgendes:

App-Typ	Verhalten bei App-Zuweisung	Verhalten bei Aufhebung der App-Zuweisung	Verhalten bei Entfernen des Geräts aus BES12
Öffentliche Apps mit Verfügbarkeitseinstellung „Erforderlich“	• Der Benutzer wird aufgefordert, die Apps zu installieren. • Die Apps werden auf der Registerkarte „Öffentliche Apps“ in BlackBerry World for Work angezeigt.	• Der Benutzer wird aufgefordert, die Apps zu deinstallieren.	• Der geschäftliche Bereich und alle geschäftlichen Apps werden automatisch entfernt.

App-Typ	Verhalten bei App-Zuweisung	Verhalten bei Aufhebung der App-Zuweisung	Verhalten bei Entfernen des Geräts aus BES12
Öffentliche Apps mit Verfügbarkeitseinstellung „Optional“	• Der Benutzer kann wählen, ob er die Apps installieren möchte. • Die Apps werden auf der Registerkarte „Öffentliche Apps“ in BlackBerry World for Work angezeigt.	• Der Benutzer wird aufgefordert, die Apps zu deinstallieren.	• Der geschäftliche Bereich und alle geschäftlichen Apps werden automatisch entfernt.
Interne Apps mit Verfügbarkeitseinstellung „Erforderlich“	• Die Apps werden automatisch auf Geräten installiert. • Der Benutzer kann die Apps nicht deinstallieren.	• Die Apps werden automatisch vom Gerät entfernt.	• Der geschäftliche Bereich und alle geschäftlichen Apps werden automatisch entfernt.
Interne Apps mit Verfügbarkeitseinstellung „Optional“	• Die Apps werden automatisch auf Geräten installiert. • Der Benutzer kann die Apps nicht deinstallieren.	• Die Apps werden automatisch vom Gerät entfernt.	• Der geschäftliche Bereich und alle geschäftlichen Apps werden automatisch entfernt.

Verhindern, dass Benutzer bestimmte iOS-, Android- und Windows Phone-Apps installieren

Sie können eine Liste von iOS-, Android- und Windows Phone-Apps erstellen, die von Benutzern nicht auf Ihren Geräten installiert werden sollen. Zum Beispiel können Sie Benutzer daran hindern, schädliche Apps oder Apps, die viele Ressourcen verbrauchen, zu installieren.

Um eine bestimmte Aktion zu erzwingen, wenn eine gesperrte App auf einem iOS- oder Android-Gerät installiert wird, das nicht Samsung KNOX MDM verwendet, müssen Sie ein Kompatibilitätsprofil erstellen und dieses Benutzern oder Benutzergruppen zuweisen. Das Kompatibilitätsprofil gibt an, welche Aktionen ausgeführt werden, wenn der Benutzer die gesperrte App nicht vom Gerät löscht. Wenn der Benutzer eine gesperrte App installiert, meldet das Gerät des Benutzers, dass diese App nicht kompatibel ist, und der Name der gesperrten App sowie die Aktionen, die ausgeführt werden, wenn die App nicht deinstalliert wird, werden im Kompatibilitätsbericht angezeigt.

Unter Windows Phone 8.1 oder höher und bei Android-Geräten, die KNOX MDM verwenden, müssen Sie die App lediglich dem Kompatibilitätsprofil hinzufügen und keine Kompatibilitätsaktionen festlegen. Grund dafür ist, dass der Benutzer daran gehindert wird, Apps zu installieren, die Sie dem Kompatibilitätsprofil hinzufügen. Wenn ein Benutzer versucht, eine verbotene App zu installieren, wird eine Meldung auf dem Gerät angezeigt, dass diese App verboten ist und nicht installiert werden kann.

Sie müssen keine Liste mit gesperrten Apps für BlackBerry 10-Geräte und Android-Geräte mit Samsung KNOX Workspace bzw. Android for Work erstellen, da Benutzer nur von Ihnen zugelassene Apps im geschäftlichen Bereich installieren können.

Schritte zur Hinderung von Benutzern an der Installation von Apps

Um Benutzer daran zu hindern, Apps zu installieren, führen Sie die folgenden Aktionen aus:

Schritt	Aktion
1	Fügen Sie die App zur Liste der gesperrten Apps hinzu.
2	Erstellen oder bearbeiten Sie ein Kompatibilitätsprofil, das die Aktionen angibt, die ausgeführt werden, wenn eine gesperrte App auf einem Gerät erstellt wird.
3	Weisen Sie das Kompatibilitätsprofil einem Benutzer, einer Benutzergruppe oder einer Gerätegruppe zu.

Hinzufügen einer App zur Liste der gesperrten Apps

Die Liste der gesperrten Apps entspricht der Bibliothek von Apps, die Benutzer nicht auf iOS-, Android- oder Windows Phone-Geräten installieren dürfen.

1. Klicken Sie in der Menüleiste auf **Apps**.
2. Klicken Sie auf **Gesperrte Apps**.
3. Klicken Sie auf +.
4. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Hinzufügen einer iOS-App zur Liste der gesperrten Apps	1. Klicken Sie auf **App Store**. 2. Suchen Sie im Suchfeld nach der App, die Sie hinzufügen möchten. Sie können nach App-Name, Anbieter oder App Store-URL suchen. 3. Klicken Sie auf **Suchen**. 4. Klicken Sie in den Suchergebnissen auf **Hinzufügen**, um eine App hinzuzufügen.

Aufgabe	Schritte
Hinzufügen einer Android-App zur Liste der gesperrten Apps	1. Klicken Sie auf **Google Play**. 2. Geben Sie im Feld **App-Name** den Namen der App ein. 3. Geben Sie im Feld **App-Webadresse von Google Play** die Webadresse der App in Google Play ein. 4. Klicken Sie auf **Hinzufügen**, um die App hinzuzufügen, oder klicken Sie auf **Hinzufügen und neu**, um eine weitere App hinzuzufügen, nachdem Sie die aktuelle App hinzugefügt haben.
Hinzufügen einer Windows Phone-App zur Liste der gesperrten Apps	1. Klicken Sie auf **Windows Phone Store**. 2. Geben Sie im Feld **App-Name** den Namen der App ein. 3. Geben Sie im Feld **App-Webadresse im Windows Phone Store** die Webadresse der App in Windows Phone Store ein. 4. Klicken Sie auf **Hinzufügen**, um die App hinzuzufügen, oder klicken Sie auf **Hinzufügen und neu**, um eine weitere App hinzuzufügen, nachdem Sie die aktuelle App hinzugefügt haben.

Verwalten von App-Gruppen

Mit App-Gruppen können Sie eine Zusammenstellung von Apps erstellen, die Benutzern, Benutzergruppen oder Gerätegruppen zugewiesen werden kann. Die Gruppierung von Apps steigert die Effizienz und Konsistenz bei der Verwaltung von Apps. Beispielsweise können Sie App-Gruppen nutzen, um die gleiche App für mehrere Gerätetypen zu gruppieren oder Apps für Benutzer mit der gleichen Rolle innerhalb Ihrer Organisation zu gruppieren.

App-Gruppen werden auch zur Verwaltung von Apps auf Android for Work-Geräten verwendet. Zum Verwalten von Apps auf Android for Work-Geräten müssen Sie die App-Gruppe für Android for Work aktivieren. Wenn Sie die App-Gruppe für Android for Work aktivieren, wird das Android for Work-Symbol im Gruppenordner in der App-Liste angezeigt. Wenn Sie eine App-Gruppe für Android for Work aktiviert haben, können Sie diese nicht als Android for Work-App-Gruppe deaktivieren. Sie können bis zu 200 App-Gruppen, die für Android for Work aktiviert sind, erstellen.

BES12 bietet eine vorkonfigurierte Android for Work-App-Gruppe namens „Empfohlene Android for Work-Apps“. Die App-Gruppe enthält den Google Chrome-Browser und Divide Productivity-Apps, Sie können der Gruppe jedoch auch Apps hinzufügen.

Erstellen einer App-Gruppe

Bevor Sie beginnen: Fügen Sie die Apps der Liste der verfügbaren Apps hinzu.

1. Klicken Sie in der Menüleiste auf **Apps**.

2. Klicken Sie auf .
3. Aktivieren Sie die Option **App-Gruppe für Android for Work aktivieren**, um eine App-Gruppe zu erstellen, die Apps umfasst, die auf Android for Work-Geräten installiert werden können. Die App-Gruppe wird auch in Ihrer Google-Domäne erstellt.
4. Geben Sie einen Namen und eine Beschreibung für die App-Gruppe ein.
5. Klicken Sie auf +.
6. Führen Sie beim Hinzufügen einer iOS-App eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Wenn Sie kein VPP-Konto hinzugefügt haben	1. Klicken Sie auf **Hinzufügen**.
Wenn Sie mindestens ein VPP-Konto hinzugefügt haben	1. Klicken Sie auf **Weiter**. 2. Wählen Sie **Ja**, wenn Sie der iOS-App eine Lizenz hinzufügen möchten. Wählen Sie **Nein**, wenn Sie keine Lizenz zuweisen möchten oder keine Lizenz haben, die Sie der App zuweisen könnten. 3. Wenn Sie der App eine Lizenz zugewiesen haben, wählen Sie in der Dropdown-Liste **App-Lizenz erteilen** das VPP-Konto aus, das mit der App verknüpft werden soll. 4. Klicken Sie auf **Hinzufügen**. Benutzer müssen sich entsprechend der Anweisungen auf ihrem Gerät im VPP Ihrer Organisation registrieren, bevor sie vorausbezahlte Apps installieren können. Benutzer müssen diese Aufgabe ein Mal erledigen. **Hinweis:** Wenn Sie mehr Lizenzen gewähren möchten, als verfügbar sind, kann der erste Benutzer, der auf die verfügbaren Lizenzen zugreift, die App installieren.

7. Wählen Sie die Apps aus, die Sie der App-Gruppe hinzufügen möchten.
8. Klicken Sie auf **Hinzufügen**.
9. Klicken Sie auf **Hinzufügen**.

Bearbeiten einer App-Gruppe

1. Klicken Sie in der Menüleiste auf **Apps**.
2. Klicken Sie auf die App-Gruppe, die Sie bearbeiten möchten.

3. Nehmen Sie die notwendigen Bearbeitungen vor.
4. Klicken Sie auf **Speichern**.

Verwalten von Apple VPP-Konten

Das Apple Volume Purchase Program (VPP) ermöglicht Ihnen, iOS-Apps in Mengen zu kaufen und zu verteilen. Sie können Apple VPP-Konten mit einer BES12 verknüpfen, sodass Sie gekaufte Lizenzen für mit VPP-Konten verknüpfte iOS-Apps verteilen können.

Hinzufügen eines Apple VPP-Kontos

1. Klicken Sie in der Menüleiste auf **Apps**.
2. Klicken Sie auf **iOS-App-Lizenzen**.
3. Klicken Sie auf **Apple VPP-Konto hinzufügen**.
4. Geben Sie einen Namen und die Kontodaten für das VPP-Konto ein.
5. Fügen Sie im Feld **VPP-Service-Token** den 64-Bit-Code aus der VPP-Token-Datei ein. Dies ist die Datei, die der VPP-Kontoinhaber aus dem VPP-Store heruntergeladen hat.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie die Apps aus, die Sie der App-Liste hinzufügen möchten. Wenn die App bereits der App-Liste hinzugefügt wurde, können Sie sie nicht auswählen, und ihr Status lautet „Bereits hinzugefügt“.
8. Wenn Sie die Apps aus den Geräten entfernen möchten, sobald die Apps aus BES12 gelöscht werden, aktivieren Sie **Die App vom Gerät entfernen, wenn das Gerät aus dem System entfernt wird**.
9. Wenn Apps auf iOS-Geräten nicht in den iCloud-Onlinedienst gesichert werden sollen, aktivieren Sie das entsprechende Kontrollkästchen. Diese Option gilt nur für Apps, deren Verfügbarkeit auf „Erforderlich“ festgelegt ist. Die Verfügbarkeit der App wird festgelegt, wenn Sie die App einem Benutzer oder einer Gruppe zuweisen.
10. Führen Sie in der Dropdown-Liste **Standardinstallationsmethode** eine der folgenden Aktionen aus:
    - Wenn Benutzer auf Ihren iOS-Geräten eine Aufforderung zur Installation der Apps erhalten sollen, wählen Sie **Einmal auffordern**. Wenn der Benutzer die Aufforderung schließt, kann er die Apps später über den Bildschirm „Geschäftliche Apps“ im BES12 Client oder über das Symbol „Geschäftliche Apps“ auf dem Gerät installieren.
    - **Keine Eingabeaufforderung**

    Die Standardinstallationsmethode gilt nur für Apps, deren Verfügbarkeit auf „Erforderlich“ festgelegt ist. Die Verfügbarkeit der App wird festgelegt, wenn Sie die App einem Benutzer oder einer Gruppe zuweisen.
11. Klicken Sie auf **Hinzufügen**.

Bearbeiten eines Apple VPP-Kontos

1. Klicken Sie in der Menüleiste auf **Apps**.
2. Klicken Sie auf **iOS-App-Lizenzen**.
3. Klicken Sie auf .
4. Bearbeiten Sie die VPP-Kontodaten.
5. Klicken Sie auf **Speichern**.

Aktualisieren der Apple VPP-Kontodaten

Wenn die Seite „App-Lizenzen“ geöffnet wird, werden die aktuellen Lizenzinformationen automatisch über die Apple VPP-Server synchronisiert. Sie können bei Bedarf die Lizenzinformationen, die Sie in BES12 hinzugefügt haben, auch manuell aktualisieren.

1. Klicken Sie in der Menüleiste auf **Apps**.
2. Klicken Sie auf **iOS-App-Lizenzen**.
3. Klicken Sie auf .

Löschen eines Apple VPP-Kontos

Bevor Sie beginnen: Entfernen Sie Apps mit verknüpften Lizenzen aus den Benutzern, bevor Sie das VPP-Konto löschen.

1. Klicken Sie in der Menüleiste auf **Apps**.
2. Klicken Sie auf **iOS-App-Lizenzen**.
3. Klicken Sie auf .
4. Klicken Sie auf **Löschen**.

Ändern, ob die App erforderlich oder optional ist

Sie können ändern, ob eine App erforderlich oder optional ist. Die Aktionen, die eintreten, wenn eine App auf erforderlich oder optional festgelegt wird, hängen von der Art der App, des Geräts und der Aktivierung ab.

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte**.
2. Wenn die zu ändernde App einem Benutzerkonto zugewiesen ist, klicken Sie in den Sucherergebnissen auf den Namen eines Benutzerkontos.
3. Wenn die zu ändernde App einer Gruppe zugewiesen ist, klicken Sie im linken Fensterbereich auf **Gruppen**, um die Liste der Benutzergruppen zu erweitern, und klicken Sie dann auf den Namen der Gruppe.
4. Klicken Sie im Abschnitt **Gruppen und Benutzern zugewiesene Apps** auf die zu ändernde Verfügbarkeit der App.
5. Wählen Sie **Optional** oder **Erforderlich** in der Dropdown-Liste **Verfügbarkeit** der App aus.

6. Klicken Sie auf **Zuweisen**.

Verwandte Informationen
App-Verhalten auf Android-Geräten, auf Seite 160
App-Verhalten auf iOS-Geräten, auf Seite 166
App-Verhalten auf BlackBerry-Geräten, auf Seite 168

Anzeigen des Status von Benutzerkonten zugewiesenen Apps und App-Gruppen

1. Klicken Sie in der Menüleiste auf **Apps**.
2. Klicken Sie unter **Benutzern zugewiesen** auf die Nummer der App oder App-Gruppe, die Sie anzeigen möchten.
3. Klicken Sie auf ***x* Benutzern zugewiesen**, um die Benutzerkonten anzuzeigen, denen diese App zugewiesen ist.
4. Prüfen Sie in der Spalte **Zugewiesen von**, ob die App oder App-Gruppe direkt dem Benutzerkonto oder einer Gruppe zugewiesen wurde.
5. Prüfen Sie in der Spalte **Status**, ob eine App auf einem Gerät installiert wurde. Folgende Status sind möglich:
    - **Installiert**: Die App wurde erfolgreich auf dem Gerät des Benutzers installiert.
    - **Nicht installiert**: Die App wurde noch nicht auf dem Gerät des Benutzers installiert.
    - **Kann nicht installiert werden**: Die App wird von den Geräten des Benutzers nicht unterstützt.
    - **Nicht unterstützt**: Das Betriebssystem des Geräts unterstützt diese App nicht.

Anzeigen, welche Apps Benutzergruppen zugewiesen wurden

1. Klicken Sie in der Menüleiste auf **Apps**.
2. Klicken Sie unter **Benutzern zugewiesen** auf die Nummer der App, die Sie anzeigen möchten.
3. Klicken Sie auf ***x* Gruppen zugewiesen**, um die Benutzergruppen anzuzeigen, denen diese App zugewiesen ist.

Aktualisieren der Daten in der Liste der verfügbaren Apps

Sie können die App-Liste aktualisieren, um sicherzustellen, dass Sie über die aktuellen Daten zu den BlackBerry 10- und iOS-Apps verfügen.

Wenn Sie eine Android for Work-Konfiguration haben, können Sie auch App-Informationen für Android-Apps aktualisieren. Wenn Sie Android-Apps vor dem Konfigurieren von Android for Work hinzugefügt haben oder App-Berechtigungen geändert wurden, müssen Sie die App-Informationen aktualisieren, damit Sie Apps für Android for Work-Geräte verfügbar machen können. Dies ist auch der Fall, wenn Sie Änderungen an der Android for Work-Verbindung vornehmen.

Informationen zu Google Play müssen manuell aktualisiert werden, wenn Sie keine Android for Work-Verbindung und Windows Phone-Apps haben. Die Aktualisierung der App-Daten bedeutet nicht, dass die App auf dem Gerät eines Benutzers aktualisiert wird. Benutzer erhalten Aktualisierungsbenachrichtigungen zu ihren geschäftlichen Apps auf die gleiche Weise wie für ihre persönlichen Apps.

1. Klicken Sie in der Menüleiste auf **Apps**.
2. Klicken Sie auf .

Aktualisieren von App-Berechtigungen für Android for Work-Apps

Wenn Sie App-Berechtigungen nicht im Namen von Benutzern annehmen, können Apps App-Gruppen, die für Android for Work aktiviert wurden, nicht hinzugefügt werden und Android for Work-Geräten nicht zugewiesen werden. App-Berechtigungen müssen beim Hinzufügen einer App zur App-Liste angenommen werden. Werden die Berechtigungen für eine App später geändert, müssen die App-Berechtigungen evtl. noch einmal angenommen werden.

Apps können auch über die Google Play for Work-Konsole als unzulässig eingestuft worden sein und dennoch in BES12 als verfügbar angezeigt werden. Sie müssen die App-Informationen in BES12 aktualisieren, um die Liste mit Google Play for Work zu synchronisieren.

1. Klicken Sie in der Menüleiste auf **Apps**.
2. Klicken Sie auf .
3. Klicken Sie auf **Schließen**.
4. In der App-Liste werden Apps, bei denen Berechtigungen geändert wurden, mit einem Warnsymbol dargestellt. Klicken Sie auf eine App mit geänderten Berechtigungen.
5. Klicken Sie auf **App-Berechtigungen anzeigen**.
6. Wählen Sie **Annehmen**.
7. Klicken Sie auf **Annehmen**.
8. Klicken Sie auf **Speichern**.

Festlegen des Organisationsnamens für BlackBerry World

Sie können den Namen Ihrer Organisation in der BlackBerry World for Work-Verkaufsplattform hinzufügen.

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Erweitern Sie **App-Verwaltung**, und klicken Sie auf **BlackBerry World for Work**.
3. Geben Sie unter **Name der Organisation** den Namen Ihrer Organisation ein.
4. Klicken Sie auf **Speichern**.

Verwalten von Apps auf BlackBerry OS-Geräten

21

Wenn die BES12-Domäne Geräte mit BlackBerry OS (Version 5.0 bis 7.1) unterstützt, können Sie die Verwaltungskonsole verwenden, um die BlackBerry Device Software- und BlackBerry Java Applications auf BlackBerry OS-Geräten zu installieren und zu verwalten.

Um BlackBerry Java Applications an BlackBerry OS-Geräte zu senden, müssen Sie die Apps zunächst im freigegebenen Netzwerkordner hinzufügen. Sie können den freigegebenen Netzwerkordner verwenden, um alle Versionen der BlackBerry Java Applications zu speichern und zu verwalten, die Sie auf Geräten installieren, aktualisieren oder von diesen entfernen möchten.

In der Verwaltungskonsole können Sie Softwarekonfigurationen erstellen, um die Versionen der BlackBerry Device Software und der BlackBerry Java Applications anzugeben, die Sie auf BlackBerry OS-Geräten installieren, aktualisieren oder von diesen entfernen möchten. Sie können Softwarekonfigurationen auch verwenden, um anzugeben, welche Apps erforderlich, optional oder nicht zulässig sind. Wenn Sie eine Softwarekonfiguration erstellen, müssen Sie auch angeben, ob Benutzer Apps installieren können, die nicht in der Softwarekonfiguration aufgeführt sind.

Wenn Sie einer Softwarekonfiguration eine BlackBerry Java Application hinzufügen, müssen Sie der App eine Richtlinie zur App-Steuerung zuweisen, um anzugeben, auf welche Ressourcen die App zugreifen kann. Sie können Standardrichtlinien zur Anwendungssteuerung verwenden, oder Sie können benutzerdefinierte Anwendungssteuerungsrichtlinien erstellen und verwenden. Wenn Sie Benutzern gestatten, nicht aufgeführte Anwendungen zu installieren, müssen Sie eine Richtlinie zur Anwendungssteuerung für nicht aufgeführte Anwendungen erstellen, die angibt, auf welche Ressourcen die Anwendungen zugreifen können.

Wenn Sie einer Benutzergruppe oder einzelnen Benutzerkonten eine Softwarekonfiguration zuweisen, erstellt die Verwaltungskonsole einen Bereitstellungsauftrag, um die BlackBerry Device Software- und BlackBerry Java Applications auf Geräten zu installieren und Anwendungssteuerungsrichtlinien auf die Geräte anzuwenden.

Weitere Informationen über das Installieren und Verwalten der BlackBerry Device Software auf BlackBerry OS-Geräten finden Sie im Aktualisierungshandbuch für die BlackBerry Device Software unter help.blackberry.com/detectlang/bes5.

Vorbereiten der Verteilung von BlackBerry Java Applications

Um eine BlackBerry Java Application an Geräte mit BlackBerry OS (Version 5.0 bis 7.1) zu senden, muss der Anwendungsentwickler eine ZIP-Datei erstellen, in der die erforderlichen Anwendungsdateien und eine ALX-Datei mit Informationen zur Anwendung enthalten sind. Falls in der ALX-Datei eine Verzeichnisstruktur beschrieben wird, muss diese Verzeichnisstruktur in der ZIP-Datei vorhanden sein.

Weitere Informationen zum Erstellen von BlackBerry Java Applications und ALX-Dateien finden Sie unter www.blackberry.com/developers. Hier können Sie das BlackBerry Java *Entwicklungshandbuch für die Entwicklungsumgebung* anzeigen.

Bevor Sie BlackBerry Java Applications verteilen, müssen Sie mithilfe der Verwaltungskonsole einen freigegebenen Netzwerkordner für BlackBerry Java Applications angeben. Weitere Informationen finden Sie unter Angeben des freigegebenen Netzwerkpfads zur Speicherung interner Apps.

Nachdem Sie eine App dem freigegebenen Netzwerkordner hinzugefügt haben, können Sie die App einer Softwarekonfiguration hinzufügen, angeben, ob die App auf BlackBerry OS-Geräten erforderlich, optional oder nicht zulässig ist, sowie der App eine Anwendungssteuerungsrichtlinie zuweisen, um die Zugriffsberechtigungen für die App zu steuern. Sie weisen Benutzerkonten Softwarekonfigurationen zu, um BlackBerry Java Applications auf BlackBerry-Geräten zu installieren oder zu aktualisieren oder um BlackBerry Java Applications von BlackBerry OS-Geräten zu entfernen.

Hinzufügen einer BlackBerry Java Application zum freigegebenen Netzwerkordner

Um eine BlackBerry Java Application an Geräte mit BlackBerry OS (Version 5.0 bis 7.1) zu senden, müssen Sie zunächst das BlackBerry Java Application-Paket im freigegebenen Netzwerkpfad hinzufügen. Um eine aktualisierte Version einer BlackBerry Java Application an BlackBerry OS-Geräte zu senden, müssen Sie zuerst das aktualisierte Paket der Anwendungsdatenbank hinzufügen. Weitere Informationen zur Einrichtung eines freigegebenen Netzwerkordners finden Sie unter Angeben des freigegebenen Netzwerkpfads zur Speicherung interner Apps.

1. Klicken Sie in der Menüleiste auf **BlackBerry OS-Einstellungen**.
2. Klicken Sie auf **Anwendungen hinzufügen oder aktualisieren**.
3. Klicken Sie im Abschnitt **Anwendungsverzeichnis** auf **Durchsuchen**. Navigieren Sie zum BlackBerry Java Application-Paket, das Sie im Anwendungsverzeichnis hinzufügen oder aktualisieren möchten.
4. Klicken Sie auf **Weiter**.
5. Klicken Sie auf **Anwendung hinzufügen**.

Angeben von Schlüsselwörtern für eine BlackBerry Java Application .

Sie können Schlüsselwörter für eine BlackBerry Java Application angeben. Diese Schlüsselwörter können Sie dazu verwenden, um in der Anwendungsdatenbank nach dieser Anwendung zu suchen.

1. Klicken Sie in der Menüleiste auf **BlackBerry OS-Einstellungen**.
2. Klicken Sie auf **Anwendungen verwalten**.
3. Suchen Sie nach einer Anwendung.
4. Klicken Sie in den Suchergebnissen auf den Namen einer Anwendung.
5. Klicken Sie auf **Anwendung bearbeiten**.
6. Geben Sie im Feld **Anwendungsschlüsselwörter** ein Schlüsselwort ein.
7. Klicken Sie auf das Symbol **Hinzufügen**.

8. Wiederholen Sie Schritt 6 und 7 für jedes Schlüsselwort, das Sie hinzufügen möchten.
9. Klicken Sie auf **Alles speichern**.

Konfigurieren von Anwendungssteuerungsrichtlinien

Wenn Sie einer Softwarekonfiguration eine BlackBerry Java Application hinzufügen, damit Sie die Anwendung auf Geräten mit BlackBerry OS (Version 5.0 bis 7.1) installieren können, müssen Sie eine Richtlinie zur Anwendungssteuerung angeben, die auf die BlackBerry Java Application angewendet werden soll. Anwendungssteuerungsrichtlinien steuern, auf welche Daten und APIs BlackBerry Java Applications auf BlackBerry OS-Geräten zugreifen können und auf welche externen Datenquellen und Netzwerkverbindungen BlackBerry Java Applications zugreifen können.

BES12 enthält eine Standardrichtlinie zur Anwendungssteuerung für BlackBerry Java Applications, die Sie als erforderlich, optional oder nicht zulässig klassifizieren können. Sie können die Standardeinstellungen der Standardrichtlinien zur Anwendungssteuerung ändern oder benutzerdefinierte Anwendungssteuerungsrichtlinien für eine BlackBerry Java Application erstellen.

Weitere Informationen zur Konfiguration der Einstellungen für Anwendungssteuerungsrichtlinien finden Sie im Referenzhandbuch für Richtlinien unter help.blackberry.com/detectlang/bes5.

Standardrichtlinien zur Anwendungssteuerung

BES12 enthält die folgenden Standardrichtlinien zur Anwendungssteuerung für Geräte mit BlackBerry OS (Version 5.0 bis 7.1).

Anwendungssteuerungsrichtlinie	Beschreibung
Standardmäßig erforderlich	Wenn Sie die Richtlinie zur Anwendungssteuerung auf eine BlackBerry Java Application anwenden, erfordern die Regeleinstellungen, dass die BlackBerry Java Application installiert wird und auf BlackBerry OS-Geräten ausgeführt werden darf. BlackBerry OS-Geräte installieren die App automatisch.
Standardmäßig optional	Wenn Sie die Richtlinie zur Anwendungssteuerung auf eine BlackBerry Java Application anwenden, machen die Regeleinstellungen die BlackBerry Java Application auf dem BlackBerry OS-Gerät optional. Benutzer können die BlackBerry Java Application auf ihren BlackBerry OS-Geräten installieren und ausführen.
Standardmäßig nicht zulässig	Wenn Sie die Richtlinie zur Anwendungssteuerung auf eine BlackBerry Java Application anwenden, verhindern die Regeleinstellungen, dass die BlackBerry Java Application auf den BlackBerry OS-Geräten installiert werden. Benutzer können die BlackBerry Java Application auf ihren BlackBerry OS-Geräten nicht installieren und ausführen.

Ändern einer Standardrichtlinie zur Anwendungssteuerung

Wenn Sie einer Softwarekonfiguration eine BlackBerry Java Application hinzufügen, müssen Sie der BlackBerry Java Application eine Richtlinie zur Anwendungssteuerung zuweisen. Basierend auf den Anforderungen der Organisationsumgebung können Sie die Standardeinstellungen für die Standardrichtlinien zur Anwendungssteuerung ändern.

1. Klicken Sie in der Menüleiste auf **BlackBerry OS-Einstellungen**.
2. Klicken Sie auf **Standardrichtlinien zur Anwendungssteuerung verwalten**.
3. Klicken Sie auf die Standardrichtlinie zur Anwendungssteuerung, die Sie ändern möchten.
4. Klicken Sie auf **Anwendungssteuerungsrichtlinie bearbeiten**.
5. Ändern Sie auf der Registerkarte der **Zugriffseinstellungen** im Abschnitt **Einstellungen** die Einstellungen für die Standardrichtlinie zur Anwendungssteuerung.
6. Klicken Sie auf **Alles speichern**.

Erstellen von benutzerdefinierten Anwendungssteuerungsrichtlinien für eine BlackBerry Java Application

Nachdem Sie eine BlackBerry Java Application dem freigegebenen Netzwerkordner hinzugefügt haben, können Sie die App so konfigurieren, dass sie die Standardrichtlinien zur Anwendungssteuerung verwendet, oder Sie können benutzerdefinierte Anwendungssteuerungsrichtlinien für die App erstellen. Wenn Sie möchten, dass eine BlackBerry Java Application benutzerdefinierte Anwendungssteuerungsrichtlinien verwendet, müssen Sie diese erstellen, bevor Sie die App einer Softwarekonfiguration hinzufügen. Wenn Sie die App einer Softwarekonfiguration hinzufügen, können Sie die benutzerdefinierte Richtlinie zur Anwendungssteuerung auswählen, die auf die Anwendung angewendet werden soll.

Wenn Sie die BlackBerry Java Application mehreren Softwarekonfigurationen hinzufügen und der BlackBerry Java Application in den verschiedenen Softwarekonfigurationen verschiedene benutzerdefinierte Anwendungssteuerungsrichtlinien zuweisen, müssen Sie die Priorität für diese festlegen. Von der Priorität wird bestimmt, welche benutzerdefinierte Anwendungssteuerungsrichtlinie der BlackBerry Policy Service anwendet, wenn Sie einem Benutzerkonto mehrere Softwarekonfigurationen zuweisen.

1. Klicken Sie in der Menüleiste auf **BlackBerry OS-Einstellungen**.
2. Klicken Sie auf **Anwendungen verwalten**.
3. Suchen Sie eine BlackBerry Java Application.
4. Klicken Sie in den Suchergebnissen auf eine BlackBerry Java Application.
5. Klicken Sie im Abschnitt **Anwendungsversionen** auf die Version der Anwendung, für die Sie eine benutzerdefinierte Richtlinie zur Anwendungssteuerung erstellen möchten.
6. Klicken Sie auf **Anwendung bearbeiten**.

7. Wählen Sie auf der Registerkarte **Anwendungssteuerungsrichtlinien** im Abschnitt **Einstellungen** die Option **Benutzerdefinierte Anwendungssteuerungsrichtlinien verwenden** aus.
8. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Erstellen Sie eine Anwendungssteuerungsrichtlinie für erforderliche BlackBerry Java Applications.	1. Geben Sie im Feld **Name der erforderlichen Anwendung** einen Namen für die Richtlinie zur Anwendungssteuerung ein. 2. Konfigurieren Sie im Abschnitt **Einstellungen** die Einstellungen für die Richtlinie zur Anwendungssteuerung. 3. Klicken Sie auf das Symbol **Hinzufügen**. 4. Wiederholen Sie die Schritte a bis c für jede Richtlinie zur Anwendungssteuerung, die Sie erstellen möchten.
Erstellen Sie eine Anwendungssteuerungsrichtlinie für optionale BlackBerry Java Applications.	1. Geben Sie im Feld **Name der optionalen Anwendung** einen Namen für die Richtlinie zur Anwendungssteuerung ein. 2. Konfigurieren Sie im Abschnitt **Einstellungen** die Einstellungen für die Richtlinie zur Anwendungssteuerung. 3. Klicken Sie auf das Symbol **Hinzufügen**. 4. Wiederholen Sie die Schritte 1 bis 3 für jede Richtlinie zur Anwendungssteuerung, die Sie erstellen möchten.
Erstellen Sie eine Anwendungssteuerungsrichtlinie für BlackBerry Java Applications, die nicht zulässig sind.	1. Geben Sie im Feld **Name der nicht zulässigen Anwendung** einen Namen für die Richtlinie zur Anwendungssteuerung ein. 2. Klicken Sie auf das Symbol **Hinzufügen**.

9. Klicken Sie ggf. in jedem Abschnitt auf den Abwärts- bzw. Aufwärtspfeil, um die Priorität für die Anwendungssteuerungsrichtlinien festzulegen.
10. Klicken Sie auf **Alles speichern**.

Rangordnung von IT-Richtlinienregeln auf BlackBerry OS-Geräten

Einstellungen der IT-Richtlinienregeln überschreiben die Einstellungen der Anwendungssteuerungsrichtlinien. Wenn Sie beispielsweise die IT-Richtlinienregel „Interne Verbindungen zulassen“ für Geräte mit BlackBerry OS (Version 5.0 bis 7.1) auf „Nein“ setzen und auf diesen Geräten eine Anwendungssteuerungsrichtlinie eingestellt ist, die einer bestimmten App das Herstellen interner Verbindungen ermöglicht, kann die App keine internen Verbindungen herstellen.

Das Gerät sperrt die Anwendungssteuerungsrichtlinie, und das Gerät wird zurückgesetzt, wenn die Berechtigungen der App, auf die diese Richtlinie angewendet wird, stärker eingeschränkt werden. Geräte ermöglichen den Benutzern die Definition stärker eingeschränkter, aber nicht weniger eingeschränkter App-Berechtigungen als die von Ihnen angegebenen Berechtigungen.

Anwendungssteuerungsrichtlinien für nicht aufgeführte Anwendungen

Wenn Sie eine Softwarekonfiguration erstellen und sie Benutzerkonten zuweisen, damit Sie BlackBerry Device Software, BlackBerry Java Applications und Standardanwendungseinstellungen an Geräte mit BlackBerry OS (Version 5.0 bis 7.1) senden können, müssen Sie konfigurieren, ob die Softwarekonfiguration Benutzern erlaubt, Apps zu installieren und zu verwenden, die nicht in der Softwarekonfiguration enthalten sind (auch bekannt als nicht aufgeführte Anwendungen). Wenn Sie konfigurieren, ob nicht aufgeführte Anwendungen auf BlackBerry OS-Geräten zulässig und optional oder nicht zulässig sind, müssen Sie der Softwarekonfiguration eine Richtlinie zur Anwendungssteuerung für nicht aufgeführte Anwendungen zuweisen.

Eine Richtlinie zur Anwendungssteuerung für nicht aufgeführte Anwendungen bestimmt, welche nicht aufgeführten Anwendungen auf BlackBerry OS-Geräten zugelassen sind und auf welche Daten die nicht aufgeführten Anwendungen auf BlackBerry OS-Geräten zugreifen können. Es gibt zwei Standardrichtlinien zur Anwendungssteuerung für nicht aufgeführte Anwendungen: eine für optionale nicht aufgeführte Anwendungen und eine für nicht zulässige nicht aufgeführte Anwendungen. Sie können die Standardeinstellungen der Standardrichtlinie zur Anwendungssteuerung für optionale nicht aufgeführte Anwendungen ändern oder benutzerdefinierte Anwendungssteuerungsrichtlinien für optionale nicht aufgeführte Anwendungen erstellen.

Ändern der Standardrichtlinie zur Anwendungssteuerung für nicht aufgeführte, optionale Anwendungen

1. Klicken Sie in der Menüleiste auf **BlackBerry OS-Einstellungen**.
2. Erweitern Sie **Software**.
3. Klicken Sie auf **Anwendungssteuerungsrichtlinien für nicht aufgeführte Anwendungen verwalten**.
4. Klicken Sie auf die Richtlinie zur Anwendungssteuerung **Standardmäßig nicht aufgelistet und optional**.
5. Klicken Sie auf **Anwendungssteuerungsrichtlinie bearbeiten**.
6. Konfigurieren Sie auf der Registerkarte der **Zugriffseinstellungen** im Abschnitt **Einstellungen** die Einstellungen für die Richtlinie zur Anwendungssteuerung.
7. Klicken Sie auf **Alles speichern**.

Erstellen einer Anwendungssteuerungsrichtlinie für nicht aufgeführte Anwendungen

Es sind zwei Standardrichtlinien zur Anwendungssteuerung für nicht aufgeführte Anwendungen vorhanden: eine für nicht aufgeführte Anwendungen, die auf Geräten mit BlackBerry OS (Version 5.0 bis 7.1) zugelassen sind, und eine für nicht aufgeführte Anwendungen, die auf BlackBerry OS-Geräten nicht ausgeführt werden dürfen. Sie können auch benutzerdefinierte Anwendungssteuerungsrichtlinien für nicht aufgeführte Anwendungen erstellen, die optional sind.

1. Klicken Sie in der Menüleiste auf **BlackBerry OS-Einstellungen**.
2. Erweitern Sie **Software**.
3. Klicken Sie auf **Anwendungssteuerungsrichtlinie für nicht aufgeführte Anwendungen erstellen**.
4. Geben Sie im Abschnitt **Informationen zu Anwendungssteuerungsrichtlinien** im Feld **Name** einen Namen für die Richtlinie zur Anwendungssteuerung für nicht aufgeführte Anwendungen ein.
5. Klicken Sie auf **Speichern**.
6. Klicken Sie im Menü **Verwaltung der BlackBerry-Lösung** auf **Anwendungssteuerungsrichtlinien für nicht aufgeführte Anwendungen verwalten**.
7. Klicken Sie auf die Richtlinie zur Anwendungssteuerung, die Sie erstellt haben.
8. Klicken Sie auf **Anwendungssteuerungsrichtlinie bearbeiten**.
9. Konfigurieren Sie auf der Registerkarte der **Zugriffseinstellungen** im Abschnitt **Einstellungen** die Einstellungen für die Richtlinie zur Anwendungssteuerung.
10. Klicken Sie auf **Alles speichern**.

Konfigurieren der Priorität der Anwendungssteuerungsrichtlinie für nicht aufgeführte Anwendungen

Sie können Benutzerkonten mehrere Softwarekonfigurationen zuweisen. Sie können verschiedenen Softwarekonfigurationen verschiedene Anwendungssteuerungsrichtlinien für nicht aufgeführte Anwendungen zuweisen. Sie müssen die Priorität der verschiedenen Anwendungssteuerungsrichtlinien für nicht aufgeführte Anwendungen konfigurieren, damit der BlackBerry Policy Service bestimmen kann, welche Anwendungssteuerungsrichtlinien auf Benutzerkonten anzuwenden sind, wenn Sie Benutzerkonten mehrere Softwarekonfigurationen zuweisen.

1. Klicken Sie in der Menüleiste auf **BlackBerry OS-Einstellungen**.
2. Erweitern Sie **Software**.
3. Klicken Sie auf **Anwendungssteuerungsrichtlinien für nicht aufgeführte Anwendungen verwalten**.
4. Klicken Sie auf **Priorität der Anwendungssteuerungsrichtlinie für nicht aufgeführte Anwendungen festlegen**.
5. Klicken Sie auf den Aufwärtspfeil bzw. den Abwärtspfeil, um die Priorität der Anwendungssteuerungsrichtlinie für nicht aufgeführte Anwendungen festzulegen.

6. Klicken Sie auf **Speichern**.

Erstellen von Softwarekonfigurationen

Mithilfe von Softwarekonfigurationen können Sie die folgenden Aktionen auf Geräten mit BlackBerry OS (Version 5.0 bis 7.1) ausführen:

- Zuweisen von Anwendungssteuerungsrichtlinien zu BlackBerry Java Applications, um Anwendungsberechtigungen zu steuern und außerdem zu steuern, auf welche Daten die Anwendung zugreifen kann
- Angeben, dass eine BlackBerry Java Application nicht zugelassen ist
- Festlegen, ob nicht in der Softwarekonfiguration enthaltene BlackBerry Java Applications zugelassen oder nicht zugelassen sind
- Konfigurieren der Zugriffsberechtigungen für BlackBerry Java Applications, die nicht in der Softwarekonfiguration enthalten sind
- Installieren oder Aktualisieren der BlackBerry Device Software über das drahtlose Netzwerk oder mithilfe von BlackBerry Web Desktop Manager
- Festlegen von Standardanwendungseinstellungen

Schritte zur Erstellung und Zuweisung einer Softwarekonfiguration

Um eine Softwarekonfiguration zu erstellen und zuzuweisen, führen Sie die folgenden Aktionen aus:

Schritt	Aktion
1	Erstellen Sie einen Netzwerkordner, und geben Sie ihn frei.
2	Fügen Sie die Anwendungen hinzu.
3	Erstellen Sie bei Bedarf eine benutzerdefinierte Anwendungssteuerungsrichtlinie.
4	Erstellen Sie eine Softwarekonfiguration.
5	Fügen Sie der Softwarekonfiguration Software hinzu.

Schritt	Aktion
6	Weisen Sie die Softwarekonfiguration einem Benutzerkonto oder einer Benutzergruppe zu.

Erstellen einer Softwarekonfiguration

1. Klicken Sie in der Menüleiste auf **BlackBerry OS-Einstellungen**.
2. Erweitern Sie **Software**.
3. Klicken Sie auf **Erstellen einer Softwarekonfiguration**.
4. Geben Sie im Abschnitt **Konfigurationsinformationen** im Feld **Name** einen Namen für die Softwarekonfiguration ein.
5. Führen Sie in der Dropdown-Liste **Verfügbarkeit für nicht aufgeführte Anwendungen** eine der folgenden Aktionen aus:
    - Um zuzulassen, dass Benutzer Anwendungen installieren, die nicht in der Softwarekonfiguration auf ihren BlackBerry OS-Geräten enthalten sind, klicken Sie auf **Optional**.
    - Um nicht zuzulassen, dass Benutzer Anwendungen installieren, die nicht in der Softwarekonfiguration auf ihren BlackBerry OS-Geräten enthalten sind, klicken Sie auf **Unzulässig**.
6. Klicken Sie in der Dropdown-Liste **Anwendungssteuerungsrichtlinie für nicht aufgeführte Anwendungen** auf die Richtlinie zur Anwendungssteuerung für nicht aufgeführte Anwendungen, die Sie der Softwarekonfiguration zuweisen möchten.
7. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Fügen Sie der Softwarekonfiguration BlackBerry Device Software-Konfigurationen und BlackBerry Java Applications hinzu.

Hinzufügen einer BlackBerry Java Application zu einer Softwarekonfiguration

Sie müssen einer Softwarekonfiguration eine BlackBerry Java Application hinzufügen und Benutzerkonten die Softwarekonfiguration zuweisen, um die BlackBerry Java Application über das drahtlose Netzwerk auf Geräten mit BlackBerry OS (Version 5.0 bis 7.1) zu installieren. Um eine Apps zu aktualisieren, müssen Sie die neue App-Version der geeigneten Softwarekonfiguration hinzufügen. BES12 aktualisiert die App auf BlackBerry OS-Geräten auf die neue Version.

1. Klicken Sie in der Menüleiste auf **BlackBerry OS-Einstellungen**.
2. Erweitern Sie **Software**.
3. Klicken Sie auf **Softwarekonfigurationen verwalten**.
4. Klicken Sie auf die Softwarekonfiguration, der Sie eine BlackBerry Java Application hinzufügen möchten.
5. Klicken Sie auf **Softwarekonfiguration bearbeiten**.

6. Klicken Sie auf der Registerkarte **Anwendungen** auf **Anwendungen zur Softwarekonfiguration hinzufügen**.
7. Suchen Sie die BlackBerry Java Applications, die Sie der Softwarekonfiguration hinzufügen möchten.
8. Wählen Sie in den Suchergebnissen eine BlackBerry Java Application aus, die Sie der Softwarekonfiguration hinzufügen möchten.
9. Führen Sie für die BlackBerry Java Application in der Dropdown-Liste **Verfügbarkeit** eine der folgenden Aktionen aus:
    - Um die BlackBerry Java Application automatisch auf BlackBerryOS-Geräten zu installieren und zu verhindern, dass Benutzer die Anwendung entfernen, klicken Sie auf **Erforderlich**.
    - Um Benutzern das Installieren und Entfernen der BlackBerry Java Application zu gestatten, wählen Sie **Optional**.
    - Um zu verhindern, dass Benutzer eine BlackBerry Java Application auf OSBlackBerry-Geräten installieren, klicken Sie auf **Unzulässig**.
10. Klicken Sie im Abschnitt **Anwendungsdaten** in der Dropdown-Liste **Anwendungssteuerungsrichtlinie** auf eine Richtlinie zur Anwendungssteuerung, um diese auf die BlackBerry Java Application anzuwenden.
11. Führen Sie in der Dropdown-Liste **Bereitstellung** eine der folgenden Aktionen aus:
    - Um die Anwendung über das drahtlose Netzwerk auf BlackBerry OS-Geräten zu installieren, klicken Sie auf **Kabellos**.
    - Um die Anwendung über eine USB-Verbindung zum Computer des Benutzers und zum BlackBerry Web Desktop Manager auf BlackBerry OS-Geräten zu installieren, klicken Sie auf **Kabel**.
12. Wiederholen Sie Schritt 6 bis 10 für jede BlackBerry Java Application, die Sie der Softwarekonfiguration hinzufügen möchten.
13. Klicken Sie auf **Zur Softwarekonfiguration hinzufügen**.
14. Klicken Sie auf **Alles speichern**.

Installieren von BlackBerry Java Applications auf einem BlackBerry OS-Gerät über einen zentralen Computer

Wenn Sie keine BlackBerry Java Applications über das drahtlose Netzwerk auf BlackBerry-Geräten installieren wollen und nicht möchten, dass der Benutzer die BlackBerry Java Applications mithilfe von BlackBerry Web Desktop Manager oder der BlackBerry Desktop Software installiert, können Sie die BlackBerry Java Applications auf einem Gerät mit BlackBerry OS (Version 5.0 bis 7.1) installieren, indem Sie das BlackBerry OS-Gerät mit einem zentralen Computer verbinden, der auf den BES12 zugreifen kann.

Bevor Sie beginnen:

- Weisen Sie dem entsprechenden Benutzerkonto eine Softwarekonfiguration mit den erforderlichen BlackBerry Java Applications zu.
- Um der Verwaltungskonsole zu gestatten, eine Verbindung zu einem BlackBerry OS-Gerät herzustellen, das mit dem Computer verbunden ist, auf dem die BES12-Verwaltungskonsole über eine USB-Verbindung gehostet wird, fügen Sie im Webbrowser die Webadresse der Verwaltungskonsole der Liste der vertrauenswürdigen Websites hinzu. Melden Sie sich erneut bei der Verwaltungskonsole an.
- Überprüfen Sie, ob der zentrale Computer auf die Verwaltungskonsole zugreifen kann.
- Verbinden Sie das dem Benutzerkonto zugeordnete BlackBerry OS-Gerät mit dem zentralen Computer.

1. Klicken Sie in der Menüleiste auf **BlackBerry OS-Einstellungen**.
2. Erweitern Sie **Angeschlossene Geräte**.
3. Klicken Sie auf **Gerätesoftware**.
4. Klicken Sie auf **Automatische Installation von Anwendungen auf dem BlackBerry-Gerät**.
5. Folgen Sie den Anweisungen auf dem Bildschirm.

Anzeigen der Benutzer, die eine BlackBerry Java Application auf ihren BlackBerry OS-Geräten installiert haben

1. Klicken Sie in der Menüleiste auf **BlackBerry OS-Einstellungen**.
2. Erweitern Sie **Software** > **Anwendungen**.
3. Klicken Sie auf **Anwendungen verwalten**.
4. Suchen Sie nach einer App.
5. Klicken Sie in den Suchergebnissen auf den Namen einer App.
6. Klicken Sie im Abschnitt **Anwendungsversionen** auf eine Version der App.
7. Klicken Sie auf **Benutzer mit Anwendung anzeigen**.
8. Suchen Sie nach Benutzern, die BlackBerry OS-Geräten zugeordnet sind, auf denen Sie die BlackBerry Java Application installiert haben.

Synchronisierungsregeln für miteinander in Konflikt stehende Einstellungen in Softwarekonfigurationen

Falls Sie Benutzerkonten oder Benutzergruppen mehrere Softwarekonfigurationen zuweisen, können die verschiedenen Softwarekonfigurationen miteinander in Konflikt stehende Einstellungen enthalten. Beispielsweise könnten Sie in einer Softwarekonfiguration, die Sie einem Benutzerkonto zuweisen, festlegen, dass eine BlackBerry Java Application erforderlich ist, aber gleichzeitig in einer anderen Softwarekonfiguration, die Sie einer Benutzergruppe zuweisen, der das Benutzerkonto angehört, festlegen, dass dieselbe Anwendung nicht zulässig ist. Konflikte können auftreten, wenn Sie mehrere BlackBerry Java Applications, Anwendungssteuerungsrichtlinien, Anwendungssteuerungsrichtlinien für nicht aufgeführte Anwendungen, BlackBerry Device Software und die Standardanwendungseinstellungen in BlackBerry Device Software-Konfigurationen zuweisen.

BES12 nutzt vordefinierte Synchronisierungsregeln zur Korrektur von in Konflikt stehenden Einstellungen bei mehreren Softwarekonfigurationen und um zu bestimmten, welche Anwendungen, Software und Einstellungen auf ein Gerät mit BlackBerry OS (Version 5.0 bis 7.1) installiert werden. BES12 löst miteinander in Konflikt stehende Einstellungen in einer asynchronen Hintergrundaktivität auf. Sie können das Ergebnis der Synchronisierungsaktivitäten, Synchronisierungsfehler und die Anwendungen, Software und Einstellungen anzeigen, die der BES12 auf einem BlackBerry OS-Gerät installiert oder auf das Gerät angewendet hat.

BES12 muss unter Umständen miteinander in Konflikt stehende Softwarekonfigurationseinstellungen synchronisieren, falls Sie eine der folgenden Aktionen ausführen:

- Aktivieren eines Geräts
- Zuweisen eines neuen BlackBerry OS-Geräts oder einer neuen PIN zu einem Benutzer
- Zuweisen eines Benutzerkontos zu einer Gruppe oder Entfernen eines Benutzerkontos aus einer Gruppe
- Hinzufügen einer Gruppe zu einer anderen Gruppe oder Entfernen einer Gruppe aus einer anderen Gruppe
- Hinzufügen einer Anwendung zu einer Softwarekonfiguration oder Entfernen einer Anwendung aus einer Softwarekonfiguration
- Ändern der Einstellungen für eine Anwendung in einer Softwarekonfiguration
- Ändern der Einstellungen für eine Anwendungssteuerungsrichtlinie
- Ändern der Rangordnung für Anwendungssteuerungsrichtlinien
- Installieren einer neuen Version der BlackBerry Device Software auf einem BlackBerry OS-Gerät
- Hinzufügen einer BlackBerry Device Software-Konfiguration zu einer Softwarekonfiguration oder Entfernen einer BlackBerry Device Software-Konfiguration aus einer Softwarekonfiguration
- Ändern einer BlackBerry Device Software-Konfiguration
- Ändern der Standardanwendungseinstellungen in einer BlackBerry Device Software-Konfiguration

Synchronisierungsregeln: BlackBerry Java Applications

Szenario	Regel
Einem Benutzerkonto oder den Gruppen, denen es angehört, werden mehrere Softwarekonfigurationen zugewiesen. In jeder Softwarekonfiguration sind mehrere BlackBerry Java Applications enthalten.	Die BlackBerry Java Applications werden auf dem Gerät mit BlackBerry OS (Version 5.0 bis 7.1) in jeder Softwarekonfiguration installiert. Falls die BlackBerry Device Software eine bestimmte BlackBerry Java Application nicht unterstützt, wird diese Anwendung nicht auf dem BlackBerry OS-Gerät installiert.
Einem Benutzerkonto oder den Gruppen, denen es angehört, werden mehrere Softwarekonfigurationen zugewiesen, die unterschiedliche Versionen der gleichen BlackBerry Java Application enthalten.	Wenn in den Softwarekonfigurationen, die einem Benutzerkonto zugewiesen sind, unterschiedliche Versionen einer App existieren, wird auf dem BlackBerry OS-Gerät die aktuelle Version der Anwendung installiert, die von der BlackBerry Device Software unterstützt wird. Wenn beispielsweise einem Benutzerkonto eine Softwarekonfiguration mit Version 1.0 einer Anwendung und eine andere Softwarekonfiguration mit Version 2.0 dieser Anwendung zugewiesen ist, wird auf dem BlackBerry OS-Gerät Version 2.0 der Anwendung installiert. Die BlackBerry Java Application-Version in einer Softwarekonfiguration, die einem Benutzerkonto zugewiesen wird, hat Vorrang vor der BlackBerry Java Application-Version in einer Softwarekonfiguration, die einer Gruppe zugewiesen wird. Wenn beispielsweise eine Softwarekonfiguration, die einem Benutzerkonto zugewiesen wird, Version 1.0 einer Anwendung enthält und einer Gruppe, der dieser Benutzer angehört, eine andere Softwarekonfiguration mit Version 2.0 dieser Anwendung zugewiesen wird, so wird auf dem BlackBerry OS-Gerät Version 1.0 der Anwendung installiert.
Einem Benutzerkonto oder den Gruppen, denen es angehört, werden mehrere Softwarekonfigurationen zugewiesen, die dieselbe BlackBerry Java Application enthalten. Die Verfügbarkeit der BlackBerry Java Application (erforderlich, optional oder unzulässig) ist in jeder Softwarekonfiguration anders eingestellt. Die Bereitstellungsmethode für die Anwendung (drahtgebunden oder über das drahtlose Netzwerk) ist in jeder Softwarekonfiguration anders eingestellt.	Die für eine Anwendung festgelegte Verfügbarkeit in einer Softwarekonfiguration, die einem Benutzerkonto zugewiesen wird, hat Vorrang vor der für die gleiche Anwendung festgelegten Verfügbarkeit in einer Softwarekonfiguration, die einer Gruppe zugewiesen wird. Falls die Anwendung in mehreren Softwarekonfigurationen, die auf der gleichen Ebene (entweder dem Benutzerkonto oder den Gruppen) zugewiesen werden, unterschiedliche Verfügbarkeiten aufweist, hat die Verfügbarkeitseinstellung „Erforderlich“ Vorrang vor der Verfügbarkeitseinstellung „Optional“ und die Verfügbarkeitseinstellung „Optional“ Vorrang vor der Verfügbarkeitseinstellung „Unzulässig“.

Szenario	Regel
	BES12 löst die Bereitstellungsmethode nach der Auflösung der Verfügbarkeit einer App auf. Die für eine App festgelegte Bereitstellungsmethode in einer Softwarekonfiguration, die einem Benutzerkonto zugewiesen wird, hat Vorrang vor der für die gleiche Anwendung festgelegten Bereitstellungsmethode in einer Softwarekonfiguration, die einer Gruppe zugewiesen wird. Die drahtlose Einstellung hat Vorrang vor der drahtgebundenen Einstellung.
Einem Benutzerkonto oder den Gruppen, denen der Benutzer angehört, sind eine oder mehrere Softwarekonfigurationen zugewiesen, die BlackBerry Java Apps enthalten, aber auf dem BlackBerry OS-Gerät bleibt eine beschränkte Menge an freiem Speicherplatz verfügbar.	BES12 prüft nach dem Auflösen von Anwendungskonflikten (beispielsweise dem Auflösen von Verfügbarkeitseinstellungen) und vor dem Installieren einer BlackBerry Java Application, wie viel Speicherplatz auf dem BlackBerry OS-Gerät verfügbar ist. Falls auf dem BlackBerry OS-Gerät nicht genug Speicherplatz verfügbar ist, um die Anwendung zu unterstützen, wird die Anwendung nicht installiert. Abhängig von der Menge an freiem Speicherplatz werden Anwendungen in folgender Reihenfolge installiert: 1. Erforderliche Apps, die für eine kabellose Bereitstellung konfiguriert sind 2. Erforderliche Apps, die für eine kabelgebundene Bereitstellung konfiguriert sind 3. Optionale Apps, die für eine kabellose Bereitstellung konfiguriert sind 4. Optionale Anwendungen, die für eine kabelgebundene Bereitstellung konfiguriert sind
Einem Benutzerkonto wird eine Softwarekonfiguration zugewiesen, in der eine BlackBerry Java Application enthalten ist, bei der eine Abhängigkeit zu einer anderen BlackBerry Java Application vorliegt.	Wenn bei einer BlackBerry Java Application in einer Softwarekonfiguration eine Abhängigkeit zu einer anderen Anwendung besteht und diese andere Anwendung nicht in einer Softwarekonfiguration enthalten ist, die dem Benutzerkonto oder einer Gruppe zugewiesen ist, der dieser Benutzer angehört, wird die Anwendung nicht auf dem BlackBerry OS-Gerät installiert. Wenn bei einer BlackBerry Java Application in einer Softwarekonfiguration eine Abhängigkeit von einer anderen App besteht und diese andere App in einer Softwarekonfiguration enthalten ist, die dem Benutzerkonto

Szenario	Regel
	oder einer Gruppe zugewiesen ist, der dieser Benutzer angehört, wird die abhängige App zuerst installiert. Wenn die abhängige App erfolgreich installiert wurde, wird die App mit der Abhängigkeit installiert.
Einem Benutzerkonto wird eine Softwarekonfiguration zugewiesen, in der eine BlackBerry Java Application enthalten ist, bei der eine Abhängigkeit zu einer anderen BlackBerry Java Application vorliegt. Die abhängige Anwendung wird auf dem BlackBerry OS-Gerät nicht unterstützt.	Wenn eine abhängige Anwendung vom BlackBerry OS-Gerät nicht unterstützt wird oder nicht erfolgreich auf dem BlackBerry OS-Gerät installiert wurde, wird die Anwendung mit der Abhängigkeit nicht auf dem BlackBerry OS-Gerät des Benutzers installiert.
Mehrere BlackBerry Java Applications weisen eine Zirkelabhängigkeit auf (Beispiel: Anwendung A ist von Anwendung B abhängig, Anwendung B ist von Anwendung C abhängig und Anwendung C ist von Anwendung A abhängig) und sind im gleichen Anwendungspaket enthalten. Das Anwendungspaket wird zur Anwendungsdatenbank hinzugefügt. Die Apps werden zu einer Softwarekonfiguration hinzugefügt und einem Benutzerkonto oder einer Gruppe zugewiesen, der dieser Benutzer angehört.	Falls mehrere BlackBerry Java Apps im gleichen Anwendungspaket enthalten sind und eine Zirkelabhängigkeit aufweisen, werden diese Anwendungen nicht auf dem BlackBerry OS-Gerät installiert. Falls mehrere Apps eine Zirkelabhängigkeit aufweisen, können sie nur installiert werden, wenn sie in separaten Anwendungspaketen enthalten sind und über eine drahtgebundene Bereitstellung installiert werden.

Synchronisierungsregeln: BlackBerry Device Software

Szenario	Regel
Einem Benutzerkonto wird eine Softwarekonfiguration zugewiesen, die BlackBerry Device Software enthält. Einer Gruppe, der das Benutzerkonto angehört, wird eine Softwarekonfiguration mit einer anderen Version der BlackBerry Device Software zugewiesen.	Die BlackBerry Device Software-Version in einer Softwarekonfiguration, die einem Benutzerkonto zugewiesen wird, hat Vorrang vor der BlackBerry Device Software-Version in einer Softwarekonfiguration, die einer Gruppe zugewiesen wird.
Einem Benutzerkonto werden mehrere Softwarekonfigurationen zugewiesen, die unterschiedliche Versionen von BlackBerry Device Software enthalten.	Auf dem BlackBerry-Gerät wird diejenige Version der BlackBerry Device Software installiert, die vom Gerät mit BlackBerry OS (Version 5.0 bis 7.1) und vom Mobilfunkanbieter unterstützt wird und der Sie in der BES12-Verwaltungskonsole den höchsten Rang zugewiesen haben. BES12 installiert eine Version der BlackBerry Device Software nicht, falls diese Version einen Rang hat, der unter dem Rang der derzeit auf dem BlackBerry OS-Gerät installierten Version der BlackBerry Device Software liegt.

Synchronisierungsregeln: Standardanwendungseinstellungen

Szenario	Regel
Einem Benutzerkonto wird eine Softwarekonfiguration mit Standardanwendungseinstellungen zugewiesen. Einer Gruppe, der das Benutzerkonto angehört, wird eine Softwarekonfiguration mit einer anderen Standardanwendungseinstellungen zugewiesen.	Die Standardanwendungseinstellungen in einer Softwarekonfiguration, die einem Benutzerkonto zugewiesen wird, hat Vorrang vor den Standardanwendungseinstellungen in einer Softwarekonfiguration, die einer Gruppe zugewiesen wird.
Ein Benutzerkonto gehört mehreren Gruppen an. Die Einstellung zur Startansicht des Kalenders wird in jeder der Softwarekonfigurationen, die den Gruppen zugewiesen wurden, anders konfiguriert.	Die Einstellung zur Startansicht des Kalenders, die auf das BlackBerry OS-Gerät (Version 5.0 bis 7.1) des Benutzers angewendet wird, ist der niedrigste Wert, der in den verschiedenen Softwarekonfigurationen festgelegt wurde.
Ein Benutzerkonto gehört mehreren Gruppen an. Die Einstellung zur Einhaltung von Kalenderterminen wird in jeder der Softwarekonfigurationen, die den Gruppen zugewiesen wurden, anders konfiguriert.	Die Einstellung zur Einhaltung von Kalenderterminen, die auf das BlackBerry OS-Gerät des Benutzers angewendet wird, ist der niedrigste Wert, der in den verschiedenen Softwarekonfigurationen festgelegt wurde.
Ein Benutzerkonto gehört mehreren Gruppen an. Die Einstellung zur Bestätigung des Löschens von E-Mails ist in einer oder mehreren der Softwarekonfigurationen, die den Gruppen zugewiesen wurden, auf „Ja“ gesetzt. In den übrigen Softwarekonfigurationen ist diese Einstellung auf „Nein“ gesetzt.	Falls die Einstellung zur Bestätigung des Löschens von E-Mails in einer Softwarekonfiguration, die einer Gruppe zugewiesen ist, der das Benutzerkonto angehört, auf „Ja“ gesetzt ist, wird diese Einstellung auf das BlackBerry OS-Gerät angewendet.
Ein Benutzerkonto gehört mehreren Gruppen an. Die E-Mail-Einstellung zum Ausblenden von gesendeten Nachrichten ist in einer oder mehreren der Softwarekonfigurationen, die den Gruppen zugewiesen wurden, auf „Ja“ gesetzt. In den übrigen Softwarekonfigurationen ist diese Einstellung auf „Nein“ gesetzt.	Falls die E-Mail-Einstellung zum Ausblenden von gesendeten Nachrichten in einer Softwarekonfiguration, die einer Gruppe zugewiesen ist, der das Benutzerkonto angehört, auf „Nein“ gesetzt ist, wird diese Einstellung auf das BlackBerry OS-Gerät angewendet.
Ein Benutzerkonto gehört mehreren Gruppen an. Die E-Mail-Einstellung zum Speichern einer Kopie im Ordner „Gesendet“ ist in einer oder mehreren der Softwarekonfigurationen, die den Gruppen zugewiesen wurden, auf „Ja“ gesetzt. In den übrigen Softwarekonfigurationen ist diese Einstellung auf „Nein“ gesetzt.	Falls die E-Mail-Einstellung zum Speichern einer Kopie im Ordner „Gesendet“ in einer Softwarekonfiguration, die einer Gruppe zugewiesen ist, der das Benutzerkonto angehört, auf „Ja“ gesetzt ist, wird diese Einstellung auf das BlackBerry OS-Gerät angewendet.
Ein Benutzerkonto gehört mehreren Gruppen an. Die Einstellung zum Sortieren des Adressbuchs wird in jeder der Softwarekonfigurationen, die den Gruppen zugewiesen wurden, anders konfiguriert.	Falls die Einstellung zum Sortieren des Adressbuchs in den Softwarekonfigurationen, die den Gruppen zugewiesen wurden, denen das Benutzerkonto angehört, unterschiedlich

Szenario	Regel
	konfiguriert sind, hat die Einstellung „Vorname“ Vorrang vor der Einstellung „Nachname“ und die Einstellung „Nachname“ Vorrang vor der Einstellung „Firmenname“.
Ein Benutzerkonto gehört mehreren Gruppen an. Die Attributeinstellungen für die verschiedenen Standardanwendungseinstellungen sind in den Softwarekonfigurationen, die den Gruppen zugewiesen wurden, unterschiedlich konfiguriert.	Die Einstellung für „Gesperrt und Sichtbar“ hat Vorrang vor der Einstellung für „Nicht gesperrt und sichtbar“. Die Einstellung für „Nicht gesperrt und Sichtbar“ hat Vorrang vor der Einstellung für „Nicht gesperrt und verborgen“.
Standardanwendungseinstellungen werden in einer Softwarekonfiguration konfiguriert und Benutzerkonten mit BlackBerry OS-Geräten zugewiesen, auf denen eine BlackBerry Device Software-Version ausgeführt wird, die älter als Version 5.0 ist.	Die Standardanwendungseinstellungen gelten nur für BlackBerry OS-Geräte mit BlackBerry Device Software Version 5.0 oder höher.

Synchronisierungsregeln: Anwendungssteuerungsrichtlinie

Szenario	Regel
Einem Benutzer werden mehrere Softwarekonfigurationen zugewiesen, die alle die gleiche Anwendung enthalten. In jeder Softwarekonfiguration wird der Anwendung eine andere Anwendungssteuerungsrichtlinie zugewiesen.	Eine Anwendungssteuerungsrichtlinie für eine Anwendung in einer Softwarekonfiguration, die einem Benutzerkonto zugewiesen wird, hat Vorrang vor einer Anwendungssteuerungsrichtlinie für die gleiche Anwendung in einer Softwarekonfiguration, die einer Gruppe zugewiesen wird. Die Einstellung „Erforderlich“ hat Vorrang vor der Einstellung „Optional“. Die Einstellung „Optional“ hat Vorrang vor der Einstellung „Unzulässig“. Wenn mehrere Softwarekonfigurationen die gleiche Anwendung enthalten und jeder Softwarekonfiguration eine andere benutzerdefinierte Anwendungssteuerungsrichtlinie mit gleicher Verfügbarkeit (zum Beispiel zwei benutzerdefinierte erforderliche Anwendungssteuerungsrichtlinien) zugewiesen wird, wird auf das BlackBerry OS-Gerät (Version 5.0 bis 7.1) des Benutzers diejenige Anwendungssteuerungsrichtlinie angewendet, der Sie in der BES12-Verwaltungskonsole den höchsten Rang zugewiesen haben.

Synchronisierungsregeln: Anwendungssteuerungsrichtlinien für nicht aufgeführte Anwendungen

Szenario	Regel
Einem Benutzerkonto wird eine Softwarekonfiguration mit einer standardmäßigen oder benutzerdefinierten Anwendungssteuerungsrichtlinie für nicht aufgeführte Anwendungen zugewiesen. Einer Gruppe, zu der das Benutzerkonto gehört, wird eine Softwarekonfiguration mit einer anderen Anwendungssteuerungsrichtlinie für nicht aufgeführte Anwendungen zugewiesen.	Die Anwendungssteuerungsrichtlinie für nicht aufgeführte Anwendungen in einer Softwarekonfiguration, die einem Benutzerkonto zugewiesen wird, hat Vorrang vor einer Anwendungssteuerungsrichtlinie für nicht aufgeführte Anwendungen in einer Softwarekonfiguration, die einer Gruppe zugewiesen wird.
Einem Benutzerkonto wird eine Softwarekonfiguration zugewiesen, die nicht aufgeführte Anwendungen als „Unzulässig“ definiert. Zusätzlich wird einem Benutzerkonto eine Softwarekonfiguration zugewiesen, die nicht aufgeführte Anwendungen als „Optional“ definiert.	Falls nicht aufgeführte Anwendungen in einer Softwarekonfiguration, die einem Benutzerkonto zugewiesen wird, als „Unzulässig“ definiert sind, werden nicht aufgeführte Anwendungen auf dem Gerät mit BlackBerry OS (Version 5.0 bis 7.1) nicht zugelassen.
Einem Benutzerkonto werden mehrere Softwarekonfigurationen mit unterschiedlichen Anwendungssteuerungsrichtlinien für nicht aufgeführte Anwendungen zugewiesen.	Auf das BlackBerry OS-Gerät wird diejenige Anwendungssteuerungsrichtlinie für nicht aufgeführte Anwendungen angewendet, der Sie in der BES12-Verwaltungskonsole den höchsten Rang zugewiesen haben.

Benutzer und Geräte

Erstellen Sie Benutzerkonten, und richten Sie Benutzer- oder Gerätegruppen ein, um Profile und Geräte gemeinsam zu verwalten.

Secure

Verwalten von Benutzergruppen und Benutzerkonten

22

Sie können Benutzerkonten und dann Benutzergruppen erstellen, um Benutzer und Geräte effizienter zu verwalten.

Schritte zur Erstellung von Benutzergruppen und Benutzerkonten

Um die Benutzer und Geräte Ihrer Organisation zu verwalten, führen Sie die folgenden Aktionen aus:

Schritt	Aktion
1	Erstellen Sie Benutzergruppen.
2	Erstellen Sie Benutzerkonten.
3	Weisen Sie Benutzergruppen und Benutzerkonten IT-Richtlinien, Profile und Apps zu.

Erstellen und Verwalten von Benutzergruppen

Eine Benutzergruppe ist eine Zusammenfassung ähnlicher Benutzer, die gemeinsame Eigenschaften haben. Die Administration von Benutzern als Gruppe ist effizienter als die Administration von individuellen Benutzern, da die Eigenschaften für alle Mitglieder der Gruppe gleichzeitig hinzugefügt, geändert oder entfernt werden können.

Benutzer können gleichzeitig zu mehr als einer Gruppe gehören. Sie können in der Verwaltungskonsole eine IT-Richtlinie, Profile und Apps zuweisen, wenn Sie die Einstellungen für eine Benutzergruppe erstellen oder aktualisieren. Wenn die BES12-Domäne BlackBerry OS-Geräte (Version 5.0 bis 7.1) unterstützt, können Sie auch eine BlackBerry OS-IT-Richtlinie, Profile und Softwarekonfigurationen zuweisen.

Sie können zwei verschiedene Arten von Benutzergruppen erstellen: per Verzeichnis verknüpfte Gruppen und lokale Gruppen. Per Verzeichnis verknüpfte Gruppen sind mit Gruppen in Ihrem Unternehmensverzeichnis verknüpft. Nur Verzeichnisbenutzerkonten können Mitglieder in einer per Verzeichnis verknüpften Gruppe sein. Lokale Gruppen werden in BES12 erstellt und verwaltet, und Sie können ihnen lokale Benutzerkonten sowie Verzeichnisbenutzerkonten zuweisen.

Nachdem Sie Benutzergruppen erstellt haben, können Sie eine Gruppe als Mitglied einer anderen Gruppe definieren. Wenn Sie eine Gruppe innerhalb einer Benutzergruppe verschachteln, übernehmen die Mitglieder der verschachtelten Gruppe die Eigenschaften der Benutzergruppe. Sie erstellen und verwalten die Verschachtelungsstruktur in BES12, und Sie können sowohl die per Verzeichnis verknüpften Gruppen als auch die lokalen Gruppen mit jeder Art von Benutzergruppe verschachteln.

Erstellen einer per Verzeichnis verknüpften Gruppe

Sie können Gruppen erstellen, die mit Gruppen in Ihrem Unternehmensverzeichnis verknüpft sind. BES12 synchronisiert die Mitgliedschaft einer per Verzeichnis verknüpften Gruppe mit ihren verknüpften Unternehmensverzeichnisgruppen, wenn die geplante Synchronisierung erfolgt. Wenn beispielsweise ein Unternehmensverzeichnis-Benutzerkonto einer Unternehmensverzeichnisgruppe hinzufügt wird, die mit einer per Verzeichnis verknüpften BES12-Gruppe verknüpft ist, wird das entsprechende BES12-Verzeichnisbenutzerkonto der per Verzeichnis verknüpften BES12-Gruppe hinzugefügt. Nur Verzeichnisbenutzerkonten können Mitglieder in einer per Verzeichnis verknüpften Gruppe sein.

Der Synchronisierungsprozess erfolgt auf der Grundlage des Zeitplans, den Sie für die Verzeichnisverbindung konfiguriert haben. Wenn die Synchronisierung nicht eingeschaltet ist, müssen Sie die Verbindung zum Unternehmensverzeichnis manuell synchronisieren, um die mit der Verzeichnisgruppe verknüpften Benutzerkonten anzuzeigen.

Wenn Onboarding für die Verzeichnisverbindung nicht aktiviert ist, müssen Sie die Benutzer in BES12 manuell erstellen, und der Synchronisierungsprozess muss erfolgen, bevor die Benutzerkonten in der Benutzerliste der per Verzeichnis verknüpften Gruppe angezeigt werden.

Sie können mehr als eine Unternehmensverzeichnisgruppe mit einer per Verzeichnis verknüpften Gruppe verknüpfen. Wenn Sie beispielsweise zwei Microsoft Active Directory-Instanzen und eine LDAP-Instanz haben, können Sie einige oder alle mit BES12 verbinden.

Eine per Verzeichnis verknüpfte Gruppe enthält nur Verknüpfungen zu Unternehmensverzeichnisgruppen aus einer einzelnen Verzeichnisverbindung. Wenn Ihr BES12 beispielsweise eine LDAP-Verzeichnisverbindung und zwei Microsoft Active Directory-Verbindungen (A und B) hat und Sie eine per Verzeichnis verknüpfte Gruppe erstellen, die mit einer Microsoft Active Directory-Verbindung A verknüpft ist, können Sie nur Unternehmensverzeichnisgruppen der Microsoft Active Directory-Verbindung A mit dieser Gruppe verknüpfen. Sie müssen neue per Verzeichnis verknüpfte Gruppen für andere Verzeichnisverbindungen erstellen.

Für jedes Unternehmensverzeichnis, das Sie mit einer per Verzeichnis verknüpften Gruppe verknüpfen, können Sie wählen, dass die Unternehmensverzeichnisverbindung die Anzahl der verschachtelten Gruppen steuert, mit denen die per Verzeichnis verknüpfte Gruppe verknüpft ist.

Informationen über die Aktivierung von per Verzeichnis verknüpften Gruppen finden Sie in der Dokumentation zur Konfiguration.

Erstellen einer per Verzeichnis verknüpften Gruppe

1. Klicken Sie in der Menüleiste auf **Gruppen**.
2. Klicken Sie auf .
3. Geben Sie den Gruppennamen ein.
4. Führen Sie im Feld **Verknüpfte Verzeichnisgruppen** eine der folgenden Aktionen aus:
   a. Klicken Sie auf +.
   b. Geben Sie den Namen oder partiellen Namen der Unternehmensverzeichnisgruppe ein, zu der Sie eine Verknüpfung erstellen möchten.
   c. Wenn mehr als eine Unternehmensverzeichnisverbindung vorhanden ist, wählen Sie diejenige aus, die Sie suchen möchten. Nach dieser Auswahl wird die per Verzeichnis verknüpfte Gruppe permanent nur mit der ausgewählten Verzeichnisverbindung verknüpft.
   d. Klicken Sie auf .
   e. Wählen Sie die Unternehmensverzeichnisgruppe in der Liste mit den Suchergebnissen aus.
   f. Klicken Sie auf **Hinzufügen**. Die Unternehmensverzeichnisgruppe wird in der Liste angezeigt, und die Unternehmensverzeichnisverbindung, mit der die Gruppe verknüpft ist, wird neben dem Titel des Abschnitts angezeigt.
   g. Aktivieren Sie ggf. das Kontrollkästchen **Verschachtelte Gruppen verknüpfen**. Um alle verschachtelten Gruppen zu verknüpfen, kann das Kontrollkästchen deaktiviert bleiben, oder Sie können das Kontrollkästchen aktivieren, damit die Verzeichniseinstellungen die Anzahl verschachtelter Gruppen steuern können.
   h. Wiederholen Sie diese Schritte, um zusätzliche Gruppen zu verknüpfen.
5. Um der per Verzeichnis verknüpften Gruppe eine IT-Richtlinie oder ein Profil zuzuweisen, führen Sie die folgenden Aktionen aus:
   a. Klicken Sie im Abschnitt **IT-Richtlinien und -Profile** auf +.
   b. Klicken Sie auf **IT-Richtlinie** oder auf einen Profiltyp.
   c. Klicken Sie in der Dropdown-Liste auf den Namen der IT-Richtlinie oder des Profils, die bzw. das Sie der Gruppe zuweisen möchten.
   d. Klicken Sie auf **Zuweisen**.
6. Wenn Sie der per Verzeichnis verknüpften Gruppe eine App zuweisen möchten, klicken Sie im Abschnitt **Zugewiesene Apps** auf +.

7. Suchen Sie nach der App.
8. Wählen Sie in den Suchergebnissen die App aus.
9. Klicken Sie auf **Weiter**.
10. Führen Sie in der Dropdown-Liste **Verfügbarkeit** der App eine der folgenden Aktionen aus:
    - Um die App automatisch auf Geräten zu installieren und zu verhindern, dass Benutzer die App entfernen, klicken Sie auf **Erforderlich**. Diese Option ist für BlackBerry-Apps nicht verfügbar.
    - Um Benutzern das Installieren und Entfernen der App zu gestatten, wählen Sie **Optional**.
11. Klicken Sie auf **Zuweisen**.
12. Klicken Sie auf **Hinzufügen**.

Erstellen einer lokalen Gruppe

1. Klicken Sie in der Menüleiste auf **Gruppen**.
2. Klicken Sie auf .
3. Geben Sie einen Namen für die Benutzergruppe ein.
4. Um der lokalen Gruppe eine IT-Richtlinie oder ein Profil zuzuweisen, führen Sie die folgenden Aktionen aus:
    a. Klicken Sie im Abschnitt **IT-Richtlinien und -Profile** auf +.
    b. Klicken Sie auf **IT-Richtlinie** oder auf einen Profiltyp.
    c. Klicken Sie in der Dropdown-Liste auf den Namen der IT-Richtlinie oder des Profils, die bzw. das Sie der Gruppe zuweisen möchten.
    d. Klicken Sie auf **Zuweisen**.
5. Wenn Sie der Benutzergruppe eine App zuweisen möchten, klicken Sie im Abschnitt **Zugewiesene Apps** auf +.
6. Suchen Sie nach der App.
7. Wählen Sie in den Suchergebnissen die App aus.
8. Klicken Sie auf **Weiter**.
9. Führen Sie in der Dropdown-Liste **Verfügbarkeit** der App eine der folgenden Aktionen aus:
    - Um die App automatisch auf Geräten zu installieren und zu verhindern, dass Benutzer die App entfernen, klicken Sie auf **Erforderlich**. Diese Option ist für BlackBerry-Apps nicht verfügbar.
    - Um Benutzern das Installieren und Entfernen der App zu gestatten, wählen Sie **Optional**.

      Hinweis: Wenn eine App gleichzeitig einem Benutzerkonto und der Benutzergruppe dieses Benutzerkontos zugewiesen ist, wird die Verfügbarkeit der App, die dem Benutzerkonto zugewiesen ist, vorrangig behandelt.
10. Klicken Sie auf **Zuweisen**.

11. Führen Sie für eine zugewiesene App – falls erforderlich – eine der folgenden Aktionen aus.
    - Klicken Sie den App-Namen, um die Details der App anzuzeigen.
    - So ändern Sie die **Verfügbarkeit** für eine App:
        1. Klicken Sie auf die Verfügbarkeit der App.
        2. Wählen Sie eine neue Verfügbarkeit aus.
        3. Klicken Sie auf **Speichern**.
    - Um eine zugewiesene App zu entfernen, klicken Sie neben der App auf ×.
12. Wenn Sie die Eigenschaften der Benutzergruppe festgelegt haben, klicken Sie auf **Hinzufügen**.

Anzeigen eines Benutzergruppe

1. Klicken Sie in der Menüleiste auf **Gruppen**.
2. Suchen Sie nach einer Benutzergruppe.
3. Klicken Sie in den Suchergebnissen auf den Namen einer Benutzergruppe.
4. Um die Mitglieder einer Benutzergruppe anzuzeigen, führen Sie die folgenden Aktionen aus:
    a. Klicken Sie auf **Benutzer**, um die zugewiesenen Benutzerkonten anzuzeigen.
    b. Klicken Sie auf **Verschachtelte Gruppen**, um die zugewiesenen verschachtelten Gruppen anzuzeigen.
5. Klicken Sie auf **Einstellungen**, um die folgenden Informationen zu einer Benutzergruppe anzuzeigen:
    - Verknüpfte Verzeichnisgruppen (verfügbar für eine per Verzeichnis verknüpfte Gruppe)
    - Zugewiesene BlackBerry OS-IT-Richtlinie, Profile und Softwarekonfigurationen (verfügbar, wenn die BES12-Domäne BlackBerry OS-Geräte unterstützt)
    - Zugewiesene IT-Richtlinien, Profile und Apps

Klicken Sie auf den Namen einer Benutzergruppe.

1. Klicken Sie in der Menüleiste auf **Gruppen**.
2. Suchen Sie die Benutzergruppe, die Sie anzeigen möchten.
3. Klicken Sie auf die Benutzergruppe.
4. Klicken Sie auf ✎.
5. Ändern Sie den Namen der Benutzergruppe.
6. Klicken Sie auf **Speichern**.

Löschen einer Benutzergruppe

1. Klicken Sie in der Menüleiste auf **Gruppen**.
2. Suchen Sie die Benutzergruppe, die Sie anzeigen möchten.
3. Klicken Sie auf die Benutzergruppe.
4. Klicken Sie auf .
5. Klicken Sie auf **Löschen**.

Hinzufügen einer Unternehmensverzeichnisgruppe zu einer vorhandenen per Verzeichnis verknüpften Gruppe

1. Klicken Sie in der Menüleiste auf **Gruppen**.
2. Klicken Sie auf die per Verzeichnis verknüpfte Gruppe.
3. Klicken Sie auf die Registerkarte **Einstellungen**.
4. Klicken Sie auf .
5. Klicken Sie im Abschnitt **Verknüpfte Verzeichnisgruppen** auf .
6. Geben Sie den Namen der Unternehmensverzeichnisgruppe ein.
7. Klicken Sie auf **Suchen**.
8. Wählen Sie die Unternehmensverzeichnisgruppe in der Liste mit den Suchergebnissen aus.
9. Klicken Sie auf **Hinzufügen**.
10. Falls erforderlich, wählen Sie **Verschachtelte Gruppen verknüpfen** aus.

Hinzufügen von verschachtelten Gruppen zu einer Benutzergruppe

Wenn Sie einer Benutzergruppe eine verschachtelte Gruppe hinzufügen, werden alle Gruppen, die dieser verschachtelten Gruppe angehören, ebenfalls hinzugefügt.

Bevor Sie beginnen: Erstellen Sie Benutzergruppen. Sie können per Verzeichnis verknüpfte Gruppen oder lokale Gruppen erstellen.

1. Klicken Sie in der Menüleiste auf **Gruppen**.
2. Suchen Sie nach einer Benutzergruppe.
3. Klicken Sie in den Suchergebnissen auf den Namen einer Benutzergruppe.
4. Klicken Sie auf die Registerkarte **Verschachtelte Gruppen**.
5. Klicken Sie auf .

6. Wählen Sie eine oder mehrere verfügbare Gruppen aus.
7. Klicken Sie auf **Hinzufügen**.

Entfernen von verschachtelten Gruppen aus einer Benutzergruppe

Sie können verschachtelte Gruppen entfernen, die einer Benutzergruppe direkt zugeordnet sind.

1. Klicken Sie in der Menüleiste auf **Gruppen**.
2. Suchen Sie nach einer Benutzergruppe.
3. Klicken Sie in den Suchergebnissen auf den Namen einer Benutzergruppe.
4. Klicken Sie auf die Registerkarte **Verschachtelte Gruppen**.
5. Klicken Sie neben der jeweiligen verschachtelten Gruppe, die Sie entfernen möchten, auf ×.

Zuweisen einer IT-Richtlinie zu einer Benutzergruppe

Bevor Sie beginnen: Erstellen Sie eine IT-Richtlinie.

1. Klicken Sie in der Menüleiste auf **Gruppen**.
2. Suchen Sie nach einer Benutzergruppe.
3. Klicken Sie in den Suchergebnissen auf den Namen einer Benutzergruppe.
4. Klicken Sie auf die Registerkarte **Einstellungen**.
5. Klicken Sie im Abschnitt **IT-Richtlinien und Profile** auf +.
6. Klicken Sie auf **IT-Richtlinie**.
7. Klicken Sie in der Dropdown-Liste auf den Namen der IT-Richtlinie, die Sie der Gruppe zuweisen möchten.
8. Wenn der Gruppe bereits direkt eine IT-Richtlinie zugewiesen ist, klicken Sie auf **Ersetzen**. Klicken Sie andernfalls auf **Zuweisen**.

Verwandte Informationen

So wählt BES12 die zuzuweisenden IT-Richtlinien aus, auf Seite 139

Zuweisen eines Profils zu einer Benutzergruppe

Bevor Sie beginnen: Erstellen Sie Profile.

1. Klicken Sie in der Menüleiste auf **Gruppen**.
2. Suchen Sie nach einer Benutzergruppe.
3. Klicken Sie in den Suchergebnissen auf den Namen einer Benutzergruppe.

4. Klicken Sie auf die Registerkarte **Einstellungen**.
5. Klicken Sie im Abschnitt **IT-Richtlinien und Profile** auf +.
6. Klicken Sie auf einen Profiltyp.
7. Klicken Sie in der Dropdown-Liste auf den Namen des Profils, das Sie der Gruppe zuweisen möchten.
8. Wenn Sie über Profiltypen mit Rangfolge verfügen und der in Schritt 6 ausgewählte Profiltyp bereits direkt der Gruppe zugewiesen ist, klicken Sie auf **Ersetzen**. Klicken Sie andernfalls auf **Zuweisen**.

Verwandte Informationen
Zuweisen von Profilen, auf Seite 58
So wählt BES12 die zuzuweisenden Profile aus, auf Seite 59

Zuweisen einer App zu einer Benutzergruppe

Wenn Sie Apps einer Benutzergruppe zuweisen, werden die Apps allen entsprechenden Geräten zur Verfügung gestellt, die die Mitglieder der Benutzergruppe aktiviert haben. Sie können Benutzergruppen auch Apps für Gerätetypen zuweisen, die die Mitglieder der Benutzergruppe noch nicht aktiviert haben. So stellen Sie sicher, dass die richtigen Apps für neue Geräte der Gruppenmitglieder zur Verfügung stehen, sobald ein Gruppenmitglied in der Zukunft einen anderen Gerätetyp aktiviert. Nur Apps in für Android for Work aktivierten App-Gruppen stehen für Android for Work-Geräte zur Verfügung. Sie können keine App für Android for Work-Geräte direkt einem Benutzerkonto oder einer Benutzergruppe zuweisen.

Wenn ein Benutzerkonto Mitglied mehrerer Benutzergruppen ist, denen die gleichen Apps oder App-Gruppen zugewiesen wurden, wird nur eine Instanz der App bzw. App-Gruppe in der Liste der zugewiesenen Apps für dieses Benutzerkonto angezeigt. Eine App kann entweder direkt einem Benutzerkonto zugewiesen werden, oder sie kann von einer Benutzergruppe oder Gerätgruppe geerbt werden. Die Einstellungen der App (ob sie beispielsweise erforderlich ist), werden entsprechend der Priorität zugewiesen: Gerätegruppen haben die höchste Priorität, gefolgt von Benutzerkonten und dann von Benutzergruppen.

Bevor Sie beginnen:

- Fügen Sie die App zur Liste der verfügbaren Apps hinzu.
- Fügen Sie die Apps optional einer App-Gruppe hinzu.
- Benutzer müssen Secure Work Space auf ihren Geräten einrichten, bevor sie zugewiesene gesicherte Apps installieren können.

1. Klicken Sie in der Menüleiste auf **Gruppen**.
2. Klicken Sie auf den Namen einer Gruppe.
3. Klicken Sie auf der Registerkarte **Einstellungen** im Abschnitt **Zugewiesene Apps** auf +.
4. Geben Sie im Suchfeld den App-Namen, den Anbieter oder die URL der App ein, die Sie hinzufügen möchten.
5. Aktivieren Sie die Kontrollkästchen neben den Apps oder der App-Gruppe, die Sie der Benutzergruppe zuweisen möchten.
6. Klicken Sie auf **Weiter**.
7. Führen Sie in der Dropdown-Liste **Verfügbarkeit** der App eine der folgenden Aktionen aus:

- Damit Benutzer die App installieren müssen, wählen Sie **Erforderlich** aus.
- Um zuzulassen, dass Benutzer die Anwendung installieren und entfernen, wählen Sie **Optional**.

  Hinweis: Wenn eine App gleichzeitig einem Benutzerkonto, der Benutzergruppe dieses Benutzerkontos und einer Gerätegruppe zugewiesen ist, wird die Verfügbarkeit der App, die der Gerätegruppe zugewiesen ist, vorrangig behandelt.

8. Wenn Sie Per App VPN-Einstellungen zu einer App-Gruppe zuweisen möchten, wählen Sie in der Dropdown-Liste **Per App VPN** die Einstellungen aus, die mit der App-Gruppe verknüpft werden sollen.
9. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Wenn Sie kein VPP-Konto hinzugefügt haben oder keine iOS-App hinzufügen	1. Klicken Sie auf **Zuweisen**.
Wenn Sie eine iOS-App hinzufügen und mindestens ein VPP-Konto hinzugefügt haben	1. Klicken Sie auf **Weiter**. 2. Wählen Sie **Ja**, wenn Sie der iOS-App eine Lizenz hinzufügen möchten. Wählen Sie **Nein**, wenn Sie keine Lizenz zuweisen möchten oder keine Lizenz haben, die Sie der App zuweisen könnten. 3. Wenn Sie der App eine Lizenz zugewiesen haben, wählen Sie in der Dropdown-Liste **App-Lizenz erteilen** das VPP-Konto aus, das mit der App verknüpft werden soll. 4. Klicken Sie auf **Zuweisen**. Benutzer müssen sich entsprechend der Anweisungen im VPP Ihrer Organisation auf ihrem Gerät registrieren, bevor sie vorausbezahlte Apps installieren können. Benutzer müssen diese Aufgabe ein Mal erledigen. **Hinweis:** Wenn Sie mehr Lizenzen gewähren möchten, als verfügbar sind, kann der erste Benutzer, der auf die verfügbaren Lizenzen zugreift, die App installieren.

Verwandte Informationen

App-Verhalten auf Android-Geräten, auf Seite 160
App-Verhalten auf iOS-Geräten, auf Seite 166
App-Verhalten auf BlackBerry-Geräten, auf Seite 168

Zuweisen einer App-Gruppe zu einer Benutzergruppe

Wenn Sie einer Benutzergruppe eine App-Gruppe zuweisen, werden die Apps in der App-Gruppe allen entsprechenden Geräten zur Verfügung gestellt, die die Mitglieder der Benutzergruppe aktiviert haben. Sie können Benutzergruppen auch Apps für Gerätetypen zuweisen, die die Mitglieder der Benutzergruppe noch nicht aktiviert haben. So stellen Sie sicher, dass die richtigen Apps für neue Geräte der Gruppenmitglieder zur Verfügung stehen, sobald ein Gruppenmitglied in der Zukunft einen anderen Gerätetyp aktiviert.

Nur Apps in für Android for Work aktivierten App-Gruppen stehen für Android for Work-Geräte zur Verfügung. Sie können keine App für Android for Work-Geräte direkt einem Benutzerkonto oder einer Benutzergruppe zuweisen.

Wenn ein Benutzerkonto Mitglied mehrerer Benutzergruppen ist, denen die gleichen App-Gruppen zugewiesen wurden, wird nur eine Instanz der App bzw. App-Gruppe in der Liste der zugewiesenen Apps für dieses Benutzerkonto angezeigt. Eine App kann entweder direkt einem Benutzerkonto zugewiesen werden, oder sie kann von einer Benutzergruppe oder Gerätegruppe geerbt werden. Die Einstellungen der App (ob sie beispielsweise erforderlich ist), werden entsprechend der Priorität zugewiesen: Gerätegruppen haben die höchste Priorität, gefolgt von Benutzerkonten und dann von Benutzergruppen.

Bevor Sie beginnen:

- Fügen Sie die Apps einer App-Gruppe hinzu.
- Benutzer müssen Secure Work Space auf ihren Geräten einrichten, bevor sie zugewiesene gesicherte Apps installieren können.

1. Klicken Sie in der Menüleiste auf **Gruppen**.
2. Klicken Sie auf den Namen einer Gruppe.
3. Klicken Sie auf der Registerkarte **Einstellungen** im Abschnitt **Zugewiesene Apps** auf +.
4. Geben Sie im Suchfeld den App-Namen, den Anbieter oder die URL der App ein, die Sie hinzufügen möchten.
5. Aktivieren Sie die Kontrollkästchen neben den Apps oder der App-Gruppe, die Sie der Benutzergruppe zuweisen möchten.
6. Klicken Sie auf **Weiter**.
7. Führen Sie in der Dropdown-Liste **Verfügbarkeit** der App eine der folgenden Aktionen aus:
    - Damit Benutzer die App installieren müssen, wählen Sie **Erforderlich** aus.
    - Um zuzulassen, dass Benutzer die Anwendung installieren und entfernen, wählen Sie **Optional**.

      Hinweis: Wenn eine App gleichzeitig einem Benutzerkonto, der Benutzergruppe dieses Benutzerkontos und einer Gerätegruppe zugewiesen ist, wird die Verfügbarkeit der App, die der Gerätegruppe zugewiesen ist, vorrangig behandelt.
8. Wenn Sie Per App VPN-Einstellungen zu einer App-Gruppe zuweisen möchten, wählen Sie in der Dropdown-Liste **Per App VPN** die Einstellungen aus, die mit der App-Gruppe verknüpft werden sollen.
9. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Wenn Sie kein VPP-Konto hinzugefügt haben oder keine iOS-App hinzufügen	1. Klicken Sie auf **Zuweisen**.
Wenn Sie eine iOS-App hinzufügen und mindestens ein VPP-Konto hinzugefügt haben	1. Klicken Sie auf **Weiter**. 2. Wählen Sie **Ja**, wenn Sie der iOS-App eine Lizenz hinzufügen möchten. Wählen Sie **Nein**, wenn Sie keine Lizenz zuweisen möchten oder keine Lizenz haben, die Sie der App zuweisen könnten. 3. Wenn Sie der App eine Lizenz zugewiesen haben, wählen Sie in der Dropdown-Liste **App-Lizenz erteilen** das VPP-Konto aus, das mit der App verknüpft werden soll. 4. Klicken Sie auf **Zuweisen**. Benutzer müssen sich entsprechend der Anweisungen im VPP Ihrer Organisation auf ihrem Gerät registrieren, bevor sie vorausbezahlte Apps installieren können. Benutzer müssen diese Aufgabe ein Mal erledigen. **Hinweis:** Wenn Sie mehr Lizenzen gewähren möchten, als verfügbar sind, kann der erste Benutzer, der auf die verfügbaren Lizenzen zugreift, die App installieren.

Verwandte Informationen

App-Verhalten auf Android-Geräten, auf Seite 160
App-Verhalten auf iOS-Geräten, auf Seite 166
App-Verhalten auf BlackBerry-Geräten, auf Seite 168

Ändern der einer Benutzergruppe zugewiesenen Per App VPN-Einstellungen

Sie können die mit einer App oder einer App-Gruppe verknüpften VPN-Einstellungen für iOS-Geräte ändern, nachdem Sie die App oder App-Gruppe dem Benutzer oder der Benutzergruppe zugewiesen haben.

1. Klicken Sie in der Menüleiste auf **Gruppen**.
2. Klicken Sie auf den Namen einer Benutzergruppe.
3. Klicken Sie auf die Registerkarte **Einstellungen**.
4. Klicken Sie im Abschnitt **Zugewiesene Apps** auf die zu ändernden Per App VPN-Einstellungen.
5. Klicken Sie im Dialogfeld **Bearbeiten der Funktion „Per App VPN“** auf die Dropdownliste **Per App VPN**, und wählen Sie die Einstellungen in der Dropdown-Liste aus.

6. Klicken Sie auf **Speichern**.

Zuweisen einer BlackBerry OS-IT-Richtlinie, eines Profils oder einer Softwarekonfiguration zu einer Benutzergruppe

Bevor Sie beginnen:

- Erstellen Sie eine BlackBerry OS-IT-Richtlinie.
- Erstellen Sie eine Softwarekonfiguration.
- Erstellen Sie ein Wi-Fi- oder VPN-Profil für BlackBerry OS-Geräte. Weitere Informationen finden Sie im Handbuch für Administratoren unter help.blackberry.com/detectLang/bes5.
- Erstellen Sie eine Push- oder Pull-Zugriffssteuerungsregel für BlackBerry OS-Geräte. Weitere Informationen finden Sie im Handbuch für Administratoren unter help.blackberry.com/detectLang/bes5.

1. Klicken Sie in der Menüleiste auf **Gruppen**.
2. Suchen Sie nach einer Benutzergruppe.
3. Klicken Sie in den Suchergebnissen auf den Namen einer Benutzergruppe.
4. Klicken Sie auf die Registerkarte **Einstellungen**.
5. Klicken Sie im Abschnitt **IT-Richtlinie, Profile und Softwarekonfigurationen** auf +.
6. Klicken Sie auf **IT-Richtlinie**, **Wi-Fi**, **VPN**, **Push einer Zugriffssteuerungsregel**, **Pull einer Zugriffssteuerungsregel** oder **Softwarekonfiguration**.
7. Klicken Sie in der Dropdown-Liste auf den Namen der IT-Richtlinie, des Profils, der Zugriffssteuerungsregel oder der Softwarekonfiguration, die bzw. das Sie der Gruppe zuweisen möchten.
8. Klicken Sie auf **Zuweisen**.

Verwandte Informationen

Zuweisen von BlackBerry OS-IT-Richtlinien und Auflösen von Konflikten zwischen IT-Richtlinien, auf Seite 146

Erstellen und Verwalten von Benutzerkonten

Sie können Benutzerkonten direkt oder über Ihr Unternehmensverzeichnis zu BES12 hinzufügen.

Wenn Sie BES12 mit Ihrem Unternehmensverzeichnis verbunden haben, können Sie ein Benutzerkonto direkt über Ihr Unternehmensverzeichnis hinzufügen. Informationen über die Aktivierung von per Verzeichnis verknüpften Gruppen finden Sie in der Dokumentation zur Konfiguration.

Sie können auch eine CSV-Datei verwenden, um BES12 mehrere Benutzerkonten gleichzeitig hinzuzufügen.

Erstellen eines Benutzerkontos

Bevor Sie beginnen: Wenn Sie einen Verzeichnisbenutzer hinzufügen möchten, stellen Sie sicher, dass BES12 mit Ihrem Unternehmensverzeichnis verbunden ist.

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte**.
2. Klicken Sie im linken Fensterbereich auf **Benutzer hinzufügen**.
3. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Hinzufügen eines Verzeichnisbenutzers	1. Geben Sie auf der Registerkarte **Unternehmensverzeichnis** im Suchfeld die Suchkriterien für den Verzeichnisbenutzer an, den Sie hinzufügen möchten. Sie können nach Vorname, Nachname, Anzeigename, Benutzername oder E-Mail-Adresse suchen. 2. Klicken Sie auf 🔍. 3. Wählen Sie in den Suchergebnissen das Benutzerkonto aus.
Hinzufügen eines lokalen Benutzers	1. Klicken Sie auf die Registerkarte **Lokal**. 2. Geben Sie im Feld **Vorname** einen Vornamen für das Benutzerkonto ein. 3. Geben Sie im Feld **Nachname** einen Nachnamen für das Benutzerkonto ein. 4. Nehmen Sie im Feld **Anzeigename** bei Bedarf die gewünschten Änderungen vor. Der Anzeigename wird automatisch anhand des von Ihnen angegebenen Vor- und Nachnamens konfiguriert. 5. Geben Sie im Feld **Benutzername** einen eindeutigen Benutzernamen für das Benutzerkonto ein. 6. Geben Sie im Feld **E-Mail-Adresse** eine Kontakt-E-Mail-Adresse für das Benutzerkonto ein.

4. Wenn in BES12 lokale Gruppen vorhanden sind und Sie das Benutzerkonto einer oder mehreren Gruppen hinzufügen möchten, wählen Sie in der Liste **Verfügbare Gruppen** die gewünschte(n) Gruppe(n) aus, und klicken Sie auf ➔.

   Wenn Sie ein Benutzerkonto erstellen, können Sie es nur lokalen Gruppen in BES12 hinzufügen. Wenn das Benutzerkonto ein Mitglied einer per Verzeichnis verknüpften Gruppe ist, wird es automatisch dieser Gruppe zugewiesen, wenn die Synchronisierung zwischen BES12 und Ihrem Unternehmensverzeichnis erfolgt.

   Zum Hinzufügen des Benutzers zu einer Benutzergruppe mit Administratorrolle müssen Sie Sicherheitsadministrator sein.

5. Wenn Sie einen lokalen Benutzer hinzufügen, geben Sie im Feld **Konsolenkennwort** ein BES12 Self-Service-Kennwort ein. Der Benutzer kann das Kennwort auch nutzen, um auf die Verwaltungskonsole zuzugreifen, falls Sie ihm eine Administratorrolle zuweisen.

6. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Automatische Generierung eines Geräteaktivierungskennworts und Senden einer E-Mail mit Aktivierungsanweisungen	1. Aktivieren Sie die Option **Automatisch ein Geräteaktivierungskennwort generieren und eine E-Mail mit Aktivierungsanweisungen senden**. 2. Legen Sie im Feld **Ablauf des Aktivierungszeitraums** die Anzahl der Minuten, Stunden oder Tage fest, innerhalb derer ein Benutzer ein Gerät vor Ablauf des Aktivierungskennworts aktivieren kann. 3. Klicken Sie in der Dropdown-Liste **Vorlage für Aktivierungs-E-Mail** auf eine Vorlage für die Aktivierungs-E-Mail für den Benutzer.
Festlegen des Geräteaktivierungskennworts	1. Aktivieren Sie die Option **Geräteaktivierungskennwort festlegen**. 2. Geben Sie ein Aktivierungskennwort ein. 3. Legen Sie im Feld **Ablauf des Aktivierungszeitraums** die Anzahl der Minuten, Stunden oder Tage fest, innerhalb derer ein Benutzer ein Gerät vor Ablauf des Aktivierungskennworts aktivieren kann. 4. Um Aktivierungsinformationen an den Benutzer zu senden, stellen Sie sicher, dass das Kontrollkästchen **E-Mail mit Aktivierungsanweisungen und Aktivierungskennwort senden** aktiviert ist. 5. Klicken Sie in der Dropdown-Liste **Vorlage für Aktivierungs-E-Mail** auf eine Vorlage für die Aktivierungs-E-Mail für den Benutzer.
Keine Festlegung des Geräteaktivierungskennworts	1. Aktivieren Sie die Option **Aktivierungskennwort für das Gerät nicht festlegen**. Sie können ein Aktivierungskennwort später festlegen und Aktivierungsanweisungen senden.

7. Wenn die BES12-Domäne Geräte mit BlackBerry OS (Version 5.0 bis 7.1) unterstützt, können Sie die BlackBerry OS-Geräteaktivierung für Verzeichnisbenutzer aktivieren bzw. deaktivieren.
   a. Aktivieren Sie das Kontrollkästchen **Benutzern erlauben, ein Gerät mit BlackBerry-Betriebssystem zu aktivieren**.

b. Klicken Sie in der Dropdown-Liste **BlackBerry OS Mail Server** auf den Namen eines Servers.

Hinweis: Der Verzeichnisbenutzer muss auf dem geschäftlichen Mailserver vorhanden sein, mit dem der BlackBerry OS-Mailserver eine Verbindung herstellt.

8. Wenn Sie benutzerdefinierte Variablen verwenden, erweitern Sie den Punkt **Benutzerdefinierte Variablen**, und geben Sie die entsprechenden Werte für die definierten Variablen ein.
9. Führen Sie eine der folgenden Aktionen aus:
   - Um Das Benutzerkonto zu speichern, klicken Sie auf **Speichern**.
   - Um das Benutzerkonto zu speichern und ein weiteres zu erstellen, klicken Sie auf **Speichern und neu**.

Verwandte Informationen
Benutzerdefinierte Variablen, auf Seite 66
Verwalten von Vorlagen für die Aktivierungs-E-Mail, auf Seite 245

Erstellen von Benutzerkonten aus einer .csv-Datei

Sie können die .csv-Datei manuell mithilfe der in BES12 enthaltenen sample.csv-Datei erstellen, die auf der Registerkarte „Import“ im Fenster „Benutzer hinzufügen“ zum Download zur Verfügung steht.

Info zur .csv-Datei mit Benutzerkonten

Sie können Benutzerkonten in einer .csv-Datei nach BES12 importieren, um viele Benutzerkonten auf einmal zu erstellen. Bei Bedarf können Sie in der .csv-Datei auch Gruppenmitgliedschaften und Aktivierungseinstellungen für die Benutzerkonten angeben, indem Sie die folgenden Spalten in der .csv-Datei aufnehmen:

Spaltenüberschrift	Beschreibung
Gruppenmitgliedschaft	Weisen Sie jedem Benutzerkonto eine oder mehrere Benutzergruppen zu. Trennen Sie mehrere Benutzergruppen mit einem Semikolon (;). Wenn Sie beim Importieren der Datei die Spalte „Gruppenmitgliedschaft“ nicht aufnehmen, haben Sie die Möglichkeit, die Gruppe auszuwählen, der alle importierten Benutzerkonten hinzugefügt werden sollen. Wenn Sie jedes Benutzerkonto einer bestimmten Benutzergruppe zuweisen möchten, verwenden Sie diese Spalte vor dem Import der Datei.
Aktivierungskennwort	Geben Sie das Aktivierungskennwort ein. Dieser Wert ist erforderlich, wenn der Wert für die „Generierung des Aktivierungskennworts“ auf „Manuell“ gesetzt ist.

Spaltenüberschrift	Beschreibung
Ablauf des Aktivierungskennworts	Geben Sie die Anzahl der Sekunden ein, für die das Aktivierungskennwort gültig ist, bevor es abläuft.
Generierung des Aktivierungskennworts	Geben Sie einen der folgenden Werte ein: • Automatisch. Das Aktivierungskennwort wird automatisch erstellt und an den Benutzer gesendet. • Manuell. Das Aktivierungskennwort wird in der Spalte „Aktivierungskennwort“ eingerichtet. Wenn Sie hier keine Angabe machen, wird der Standardwert „Automatisch“ verwendet.
Senden der Aktivierungs-E-Mail	Geben Sie einen der folgenden Werte ein: • True. Die Aktivierungs-E-Mail wird an den Benutzer gesendet. • False. Die Aktivierungs-E-Mail wird nicht an den Benutzer gesendet. Wenn „Generierung des Aktivierungskennworts“ auf „Automatisch“ gesetzt ist, wird die Aktivierungs-E-Mail unabhängig vom Wert in dieser Spalte an den Benutzer gesendet. Wenn der Wert „Generierung des Aktivierungskennworts“ auf „Manuell“ gesetzt ist und der Wert leer ist, gilt der Standardwert „Richtig“.
Benutzertyp	Diese Spalte ist immer dann erforderlich, wenn die .csv-Datei sowohl lokale Benutzerkonten als auch Verzeichnisbenutzerkonten enthält. Geben Sie einen der folgenden Werte ein: • „L“ für lokale Benutzerkonten • „D“ für Verzeichnisbenutzerkonten
Verzeichnis-UID	(Optional) Eine Alternative zum Eingeben der E-Mail-Adresse für Verzeichnisbenutzerkonten. Standardmäßig wird die E-Mail-Adresse zum Überprüfen der Verzeichnisbenutzerkonten verwendet. Sie können jedoch angeben, dass stattdessen die Verzeichnis-UID verwendet werden soll. Wenn das Benutzerkonto nicht anhand der Verzeichnis-UID überprüft werden kann, wird ein Fehler gemeldet.

Dies ist ein Beispiel der .csv-Datei:

```
Username, First name, Last name, Display name, Contact email, Group membership,
Activation password, Activation Password Expiration, Activation Password Generation,
Send activation email, User Type
JJones1, Justin1, Jones, Justin1 Jones, JJones01@example.com, Sales, password, 172800,
```

```
manual, true, d
JJones2, Justin2, Jones, Justin2 Jones, JJones02@example.com, Sales;Pre Sales, , ,
auto, true, l
JJones3, Justin3, Jones, Justin3 Jones, JJones03@example.com, Sales;Pre Sales,
password, 172800, manual, true, d
JJones4, Justin4, Jones, Justin4 Jones, JJones04@example.com, Sales, password, 172800,
manual, true, d
```

So überprüft BES12 die .csv-Datei mit Benutzerkonten

BES12 überprüft die .csv-Datei mit Benutzerkonten vor, während und sofort nach dem Laden der .csv-Datei und meldet aufgetretene Fehler.

Folgende Fehler können unter Umständen verhindern, dass BES12 die .csv-Datei lädt:

- Ein ungültiges Dateiformat oder eine ungültige Dateierweiterung
- Keine Daten in der Datei
- Die Anzahl der Spalten entspricht nicht der Anzahl an Überschriften in der Datei

Wenn BES12 einen Fehler feststellt, wird das Laden der Datei angehalten und eine Fehlermeldung angezeigt. Sie müssen den Fehler korrigieren und die .csv-Datei dann neu laden.

Nach dem Laden der .csv-Datei zeigt BES12 eine Liste mit Benutzerkonten an, die importiert werden, und ggf. die Verzeichnisbenutzerkonten, die aufgrund eines Fehlers (z. B. ein doppelter Eintrag oder eine ungültige E-Mail-Adresse) nicht importiert werden. Folgende Optionen sind möglich:

- Brechen Sie den Vorgang ab, korrigieren Sie die Fehler, und laden Sie die .csv-Datei dann neu.
- Fahren Sie fort, und laden Sie die gültigen Benutzerkonten. Verzeichnisbenutzerkonten mit Fehlern werden nicht geladen. Sie müssen die Verzeichnisbenutzerkonten, die nicht geladen wurden, in eine separate .csv-Datei kopieren und korrigieren. Andernfalls führt das erneute Laden derselben .csv-Datei zu Duplikationsfehlern für die Benutzerkonten, die erfolgreich geladen wurden.

BES12 führt vor dem Erstellen der Benutzerkonten eine letzte Überprüfung der importierten Benutzerkonten durch, um sicherzustellen, dass beim Importieren der Datei keine Fehler übernommen wurden (zum Beispiel: ein anderer Administrator hat ein Benutzerkonto zu dem Zeitpunkt erstellt, als eine .csv-Datei, die dasselbe Benutzerkonto enthielt, importiert wurde).

Hinzufügen von Benutzerkonten mithilfe einer .csv-Datei

Bevor Sie beginnen:

- Wenn die .csv-Datei Verzeichnisbenutzerkonten enthält, überprüfen Sie, ob BES12 mit Ihrem Unternehmensverzeichnis verbunden ist.
- Überprüfen Sie, ob die Anzahl der Spalten der Anzahl an Überschriften in der .csv-Datei entspricht.
- Überprüfen Sie, ob die erforderlichen Spalten vorhanden sind.
- Überprüfen Sie, ob die Informationen in den Spalten richtig sind.

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte**.

2. Klicken Sie im linken Fensterbereich auf **Benutzer hinzufügen**.
3. Klicken Sie auf die Registerkarte **Import**.
4. Klicken Sie auf **Durchsuchen**, und navigieren Sie zu der .csv-Datei mit den Benutzerkonten, die Sie hinzufügen möchten.
5. Klicken Sie auf **Laden**.
6. Falls Fehler gemeldet werden, führen Sie die folgenden Aktionen aus:
   a. Korrigieren Sie die Fehler in der .csv-Datei.
   b. Klicken Sie auf **Durchsuchen**, und navigieren Sie zu der .csv-Datei.
   c. Klicken Sie auf **Laden**.
   d. Wiederholen Sie Schritt 6, bis alle Fehler korrigiert sind.
7. Wenn die .csv-Datei die Spalte „Gruppenmitgliedschaft“ nicht verwendet und lokale Gruppen in BES12 vorhanden sind, führen Sie folgende Aktionen aus, wenn Sie den Gruppen Benutzerkonten hinzufügen möchten:
   a. Wählen Sie in der Liste **Verfügbare Gruppen** eine oder mehrere Gruppen aus, und klicken Sie auf ➔.
   b. Klicken Sie auf **Weiter**.

   Wenn Sie die .csv-Datei importieren, werden alle Benutzerkonten den von Ihnen ausgewählten lokalen Gruppen hinzugefügt. Wenn ein Benutzerkonto ein Mitglied einer per Verzeichnis verknüpften Gruppe ist, wird es automatisch dieser Gruppe zugewiesen, wenn die Synchronisierung zwischen BES12 und Ihrem Unternehmensverzeichnis erfolgt.
8. Überprüfen Sie die Liste der Benutzerkonten, und führen Sie eine der folgenden Aktionen aus:
   - Um Fehler für ungültige Verzeichnisbenutzerkonten zu korrigieren, klicken Sie auf **Abbrechen**, und fahren Sie mit Schritt 6 fort.
   - Zum Hinzufügen der gültigen Benutzerkonten klicken Sie auf **Import**. Ungültige Verzeichnisbenutzerkonten werden ignoriert.

Wenn Sie fertig sind: Wenn die BES12-Domäne BlackBerry OS-Geräte (Version 5.0 bis 7.1) unterstützt, bearbeiten Sie die Benutzerkontodaten, um die BlackBerry OS-Geräteaktivierung für Verzeichnisbenutzerkonten zu aktivieren.

Anzeigen eines Benutzerkontos

Sie können Informationen zu einem Benutzerkonto auf der Registerkarte „Benutzerzusammenfassung“ einsehen. Sie können beispielsweise folgende Informationen anzeigen:

- Aktivierte Geräte
- Benutzergruppen, denen ein Benutzerkonto angehört
- Zugewiesene BlackBerry OS-IT-Richtlinien, -Profile und -Softwarekonfigurationen (verfügbar, wenn die BlackBerry OS-Geräteaktivierung für ein Benutzerkonto aktiviert wurde)
- Zugewiesene IT-Richtlinien, Profile und Apps

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte**.

2. Suchen Sie nach einem Benutzerkonto.
3. Klicken Sie in den Suchergebnissen auf den Namen eines Benutzerkontos.

Senden einer E-Mail an einen Benutzer

Sie können direkt über die Verwaltungskonsole E-Mail-Nachrichten an eine Person senden. Der Benutzer muss über ein Konto mit einer verknüpften E-Mail-Adresse verfügen.

Die Nachricht wird von der E-Mail-Adresse gesendet, die Sie in den SMTP-Einstellungen konfiguriert haben.

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte**.
2. Suchen Sie nach einem Benutzerkonto.
3. Klicken Sie in den Suchergebnissen auf den Namen eines Benutzerkontos.
4. Klicken Sie unter dem Benutzernamen oben auf dem Bildschirm auf **Nachricht senden**.
5. Klicken Sie optional auf **CC**, und geben Sie eine oder mehrere, durch Komma oder Semikolon getrennte E-Mail-Adressen ein, um die E-Mail auch an Sie selbst oder andere zu senden.
6. Geben Sie einen Betreff und eine Nachricht ein.
7. Klicken Sie auf **Senden**.

Bearbeiten von Benutzerkontodaten

Sie können die Benutzergruppenmitgliedschaft für Verzeichnis- und lokale Benutzerkonten bearbeiten, die Mitgliedschaft von per Verzeichnis verknüpften Gruppen kann jedoch nicht geändert werden. Wenn Sie benutzerdefinierte Variablen verwenden, können Sie zudem Variableninformationen für Verzeichnis- und lokale Benutzerkonten bearbeiten. Sie können den Namen, Benutzernamen, die Kontakt-E-Mail-Adresse und das Konsolenkennwort von lokalen Benutzerkonten bearbeiten.

Wenn die BES12-Domäne Geräte mit BlackBerry OS (Version 5.0 bis 7.1) unterstützt, können Sie die BlackBerry OS-Geräteaktivierung für Verzeichnisbenutzerkonten aktivieren bzw. deaktivieren. Sie können die BlackBerry OS-Geräteaktivierung nur dann deaktivieren, wenn der Benutzer kein BlackBerry OS-Gerät aktiviert hat.

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte**.
2. Suchen Sie nach einem Benutzerkonto.
3. Klicken Sie in den Suchergebnissen auf den Namen eines Benutzerkontos.
4. Klicken Sie auf der Registerkarte **Benutzerzusammenfassung** im Abschnitt **Benutzerdaten** auf ✎.
5. Bearbeiten Sie die Benutzerkontodaten.
6. Klicken Sie auf **Speichern**.

Aktualisieren von Benutzerkontodaten

Wenn Sie ein Benutzerkonto über das Unternehmensverzeichnis hinzugefügt haben, können Sie die Daten dieses Benutzers manuell mit dem Unternehmensverzeichnis synchronisieren, statt den automatischen Synchronisierungszeitpunkt abzuwarten.

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte**.
2. Suchen Sie nach einem Benutzerkonto.
3. Klicken Sie in den Suchergebnissen auf den Namen eines Benutzerkontos.
4. Klicken Sie auf .

Ändern der Synchronisierung von Terminplanerdaten und Nachrichtenkonfiguration für einen BlackBerry OS-Gerätebenutzer

In den erweiterten Einstellungen auf der Registerkarte „Benutzerzusammenfassung“ können Sie die Einstellungen der Synchronisierung von Terminplanerdaten für ein Benutzerkonto ändern. Außerdem können Sie die Weiterleitung von Nachrichten verwalten und steuern, welche Ordner ein Benutzer auf einem BlackBerry OS-Gerät synchronisieren kann, sowie Signaturen und Haftungsausschlüsse in E-Mail-Nachrichten verwalten.

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte**.
2. Suchen Sie nach einem Benutzerkonto.
3. Klicken Sie in den Suchergebnissen auf den Namen eines Benutzerkontos.
4. Klicken Sie auf dem Register **Benutzerzusammenfassung** im Abschnitt **IT-Richtlinie, Profile und Softwarekonfigurationen** auf **Erweiterte Einstellungen**.
5. Klicken Sie auf **Benutzer bearbeiten**.
6. Klicken Sie im Abschnitt **Nachrichtenkonfiguration** auf **Standardkonfiguration**.
7. Nehmen Sie auf den entsprechenden Registerkarten Änderungen vor.
8. Klicken Sie auf **Mit Bearbeiten von Benutzerinformationen fortfahren**.
9. Klicken Sie auf **Alles speichern**.

Löschen eines Benutzerkontos

Wenn Sie ein Benutzerkonto löschen, werden auch alle geschäftlichen Daten von allen Geräten des Benutzers gelöscht.

Bevor Sie beginnen: Löschen Sie alle aktivierten Geräte, die mit dem zu löschenden Konto verknüpft sind.

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte**.
2. Suchen Sie nach einem Benutzerkonto.

3. Wählen Sie in den Suchergebnissen den Namen des Benutzerkontos aus.
4. Klicken Sie auf .
5. Klicken Sie auf **Löschen**.

Hinzufügen von Benutzern zu Benutzergruppen

Hinweis: Zum Hinzufügen eines Benutzers, dem eine Administratorrolle zugewiesen ist, zu einer Benutzergruppe müssen Sie Sicherheitsadministrator sein.

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte**.
2. Aktivieren Sie das Kontrollkästchen neben den Benutzern, die Sie den Benutzergruppen hinzufügen möchten.
3. Klicken Sie auf .
4. Wählen Sie in der Liste **Verfügbare Gruppen** eine oder mehrere Gruppen aus, und klicken Sie auf .

   Hinweis: Die Mitgliedschaft in Gruppen, die per Verzeichnis verknüpft sind, kann nicht geändert werden.
5. Klicken Sie auf **Speichern**.

Ändern der Benutzerzuweisung zu Benutzergruppen

Hinweis: Zum Ändern der Benutzergruppen, denen ein Benutzer mit Administratorrolle zugewiesen ist, müssen Sie Sicherheitsadministrator sein.

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte**.
2. Suchen Sie nach einem Benutzerkonto.
3. Klicken Sie in den Suchergebnissen auf den Namen eines Benutzerkontos.
4. Klicken Sie auf der Registerkarte **Benutzerzusammenfassung** im Abschnitt **Gruppenmitgliedschaft** auf .
5. Führen Sie eine der folgenden Aktionen aus:
   - Zum Hinzufügen des Benutzers zu Benutzergruppen wählen Sie in der Liste **Verfügbare Gruppen** eine oder mehrere Gruppen aus, und klicken Sie auf .
   - Zum Entfernen des Benutzers aus Benutzergruppen wählen Sie in der Liste **Mitglied von Gruppen** eine oder mehrere Gruppen aus, und klicken Sie auf .

   Hinweis: Die Mitgliedschaft in Gruppen, die per Verzeichnis verknüpft sind, kann nicht geändert werden.
6. Klicken Sie auf **Speichern**.

Entfernen eines Benutzers aus einer Benutzergruppe

Sie können einen Benutzer aus einer per Verzeichnis verknüpften Gruppe nicht entfernen.

Hinweis: Zum Entfernen eines Benutzers mit Administratorrolle aus einer Benutzergruppe müssen Sie Sicherheitsadministrator sein.

1. Klicken Sie in der Menüleiste auf **Gruppen**.
2. Suchen Sie die Benutzergruppe, die Sie bearbeiten möchten.
3. Klicken Sie auf die Benutzergruppe.
4. Suchen Sie den Benutzer, den Sie entfernen möchten.
5. Wählen Sie den Benutzer aus.
6. Klicken Sie auf .

Zuweisen einer IT-Richtlinie zu einem Benutzerkonto

Bevor Sie beginnen: Erstellen Sie eine IT-Richtlinie.

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte**.
2. Suchen Sie nach einem Benutzerkonto.
3. Klicken Sie in den Suchergebnissen auf den Namen eines Benutzerkontos.
4. Klicken Sie auf dem Register **Benutzerzusammenfassung** im Abschnitt **IT-Richtlinien und -Profile** auf +.
5. Klicken Sie auf **IT-Richtlinie**.
6. Klicken Sie in der Dropdown-Liste auf den Namen der IT-Richtlinie, die Sie dem Benutzer zuweisen möchten.
7. Wenn dem Benutzer bereits direkt eine IT-Richtlinie zugewiesen ist, klicken Sie auf **Ersetzen**. Klicken Sie andernfalls auf **Zuweisen**.

Verwandte Informationen

So wählt BES12 die zuzuweisenden IT-Richtlinien aus, auf Seite 139

Zuweisen eines Profils zu einem Benutzerkonto

Bevor Sie beginnen: Erstellen Sie Profile.

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte**.
2. Suchen Sie nach einem Benutzerkonto.
3. Klicken Sie in den Suchergebnissen auf den Namen eines Benutzerkontos.
4. Klicken Sie auf dem Register **Benutzerzusammenfassung** im Abschnitt **IT-Richtlinien und -Profile** auf +.
5. Klicken Sie auf einen Profiltyp.
6. Klicken Sie in der Dropdown-Liste auf den Namen des Profils, das Sie dem Benutzer zuweisen möchten.
7. Wenn Sie über Profiltypen mit Rangfolge verfügen und der in Schritt 5 ausgewählte Profiltyp bereits dem Benutzer zugewiesen ist, klicken Sie auf **Ersetzen**. Klicken Sie andernfalls auf **Zuweisen**.

Verwandte Informationen
Zuweisen von Profilen, auf Seite 58
So wählt BES12 die zuzuweisenden Profile aus, auf Seite 59

Hinzufügen eines Client-Zertifikats zu einem Benutzerkonto

Wenn die Geräte eine zertifikatbasierte Authentifizierung nutzen, um eine Verbindung zu einem Netzwerk oder Server in der Organisationsumgebung herzustellen, sollten Sie die Client-Zertifikate möglicherweise an die Geräte verteilen. Je nach Geräteaktivierungsart können Sie einem einzelnen Benutzerkonto ein Client-Zertifikat hinzufügen und dieses Zertifikat an die iOS- und Android-Geräte des Benutzers senden. Diese Option wird von Geräten mit MDM-Steuerelemente-Aktivierung, Samsung KNOX-Geräten und Android for Work-Geräten unterstützt.

Client-Zertifikate müssen über die Dateierweiterung .pfx oder .p12 verfügen. Sie können mehr als ein Client-Zertifikat an Geräte senden.

Wenn Ihr Unternehmen einen SCEP-Dienst nutzt, können Sie auch SCEP-Profile verwenden, um Client-Zertifikate auf BlackBerry 10-Geräten, iOS-Geräten und Android-Geräten mit Secure Work Space-, KNOX Workspace- oder KNOX MDM-Aktivierung zu registrieren.

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte**.
2. Suchen Sie nach einem Benutzerkonto.
3. Klicken Sie in den Suchergebnissen auf den Namen eines Benutzerkontos.
4. Klicken Sie im Abschnitt **IT-Richtlinien und Profile** auf +.
5. Klicken Sie auf **Benutzerzertifikat**.
6. Geben Sie einen Namen und eine Beschreibung für das Zertifikat ein.
7. Geben Sie im Feld **Kennwort** ein Kennwort für das Zertifikat ein.
8. Klicken Sie im Feld **Zertifikatsdatei** auf **Durchsuchen**, um die Zertifikatsdatei zu finden.
9. Klicken Sie auf **Hinzufügen**.

Verwandte Informationen
Senden von Zertifikaten an Geräte, auf Seite 71
Erstellen von SCEP-Profilen, auf Seite 73

Zuweisen einer App zu einem Benutzerkonto

Wenn Sie Apps auf Benutzerebene steuern müssen, können Sie Apps oder App-Gruppen bestimmten Benutzerkonten zuweisen. Wenn Sie eine App einem Benutzer zuweisen, wird diese App allen Geräten zur Verfügung gestellt, die der Benutzer für den entsprechenden Gerätetyp aktiviert hat. Die App wird dann im Katalog der geschäftlichen Apps auf dem Gerät aufgeführt. Nur Apps in für Android for Work aktivierten App-Gruppen stehen für Android for Work-Geräte zur Verfügung. Sie können keine App für Android for Work-Geräte direkt einem Benutzerkonto zuweisen.

Sie können Benutzern auch Apps für Gerätetypen zuweisen, die er noch nicht aktiviert hat. So stellen Sie sicher, dass die richtigen Apps für ein neues Gerät des Benutzers zur Verfügung stehen, sobald er in der Zukunft einen anderen Gerätetyp aktiviert.

Eine App kann entweder direkt einem Benutzerkonto zugewiesen werden, oder sie kann von einer Benutzergruppe oder Gerätgruppe geerbt werden. Die Einstellungen der App (ob sie beispielsweise erforderlich ist), werden entsprechend der Priorität zugewiesen: Gerätegruppen haben die höchste Priorität, gefolgt von Benutzerkonten und dann von Benutzergruppen.

Bevor Sie beginnen:

- Fügen Sie die App zur Liste der verfügbaren Apps hinzu.
- Fügen Sie die Apps optional einer App-Gruppe hinzu.
- Benutzer müssen Secure Work Space auf ihren Geräten einrichten, bevor sie zugewiesene gesicherte Apps installieren können.

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte**.
2. Suchen Sie nach einem Benutzerkonto.
3. Klicken Sie in den Suchergebnissen auf den Namen eines Benutzerkontos.
4. Klicken Sie im Abschnitt **Gruppen und Benutzern zugewiesene Apps** auf +.
5. Aktivieren Sie die Kontrollkästchen neben den Apps oder der App-Gruppe, die Sie dem Benutzerkonto zuweisen möchten.
6. Klicken Sie auf **Weiter**.
7. Führen Sie in der Dropdown-Liste **Verfügbarkeit** der App eine der folgenden Aktionen aus:
    - Damit Benutzer die App installieren müssen, wählen Sie **Erforderlich** aus.
    - Um zuzulassen, dass Benutzer die Anwendung installieren und entfernen, wählen Sie **Optional**.

      Hinweis: Wenn eine App gleichzeitig einem Benutzerkonto, der Benutzergruppe dieses Benutzerkontos und einer Gerätegruppe zugewiesen ist, wird die Verfügbarkeit der App, die der Gerätegruppe zugewiesen ist, vorrangig behandelt.
8. Wenn Sie Per App VPN-Einstellungen zu einer App zuweisen möchten, wählen Sie in der Dropdown-Liste **Per App VPN** die Einstellungen aus, die mit der App verknüpft werden sollen.
9. Führen Sie beim Hinzufügen einer iOS-App eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Wenn Sie kein VPP-Konto hinzugefügt haben oder keine iOS-App hinzufügen	1. Klicken Sie auf **Zuweisen**.
Wenn Sie eine iOS-App hinzufügen und mindestens ein VPP-Konto hinzugefügt haben	1. Klicken Sie auf **Weiter**. 2. Wählen Sie **Ja**, wenn Sie der iOS-App eine Lizenz hinzufügen möchten. Wählen Sie **Nein**, wenn Sie

Aufgabe	Schritte
	keine Lizenz zuweisen möchten oder keine Lizenz haben, die Sie der App zuweisen könnten. 3. Wenn Sie der App eine Lizenz zugewiesen haben, wählen Sie in der Dropdown-Liste **App-Lizenz erteilen** das VPP-Konto aus, das mit der App verknüpft werden soll. 4. Klicken Sie auf **Zuweisen**. Benutzer müssen sich entsprechend der Anweisungen im VPP Ihrer Organisation auf ihrem Gerät registrieren, bevor sie vorausbezahlte Apps installieren können. Benutzer müssen diese Aufgabe ein Mal erledigen. **Hinweis:** Wenn Sie mehr Lizenzen gewähren möchten, als verfügbar sind, kann der erste Benutzer, der auf die verfügbaren Lizenzen zugreift, die App installieren.

Verwandte Informationen
App-Verhalten auf Android-Geräten, auf Seite 160
App-Verhalten auf iOS-Geräten, auf Seite 166
App-Verhalten auf BlackBerry-Geräten, auf Seite 168

Zuweisen einer App oder App-Gruppe zu einem Benutzerkonto

Wenn Sie Apps auf Benutzerebene steuern müssen, können Sie Apps oder App-Gruppen bestimmten Benutzerkonten zuweisen. Wenn Sie eine App einem Benutzer zuweisen, wird diese App allen Geräten zur Verfügung gestellt, die der Benutzer für den entsprechenden Gerätetyp aktiviert hat. Die App wird dann im Katalog der geschäftlichen Apps auf dem Gerät aufgeführt. Nur Apps in für Android for Work aktivierten App-Gruppen stehen für Android for Work-Geräte zur Verfügung. Sie können keine App für Android for Work-Geräte direkt einem Benutzerkonto zuweisen.

Sie können Benutzern auch Apps für Gerätetypen zuweisen, die er noch nicht aktiviert hat. So stellen Sie sicher, dass die richtigen Apps für ein neues Gerät des Benutzers zur Verfügung stehen, sobald er in der Zukunft einen anderen Gerätetyp aktiviert.

Eine App kann entweder direkt einem Benutzerkonto zugewiesen werden, oder sie kann von einer Benutzergruppe oder Gerätegruppe geerbt werden. Die Einstellungen der App (ob sie beispielsweise erforderlich ist), werden entsprechend der Priorität zugewiesen: Gerätegruppen haben die höchste Priorität, gefolgt von Benutzerkonten und dann von Benutzergruppen.

Bevor Sie beginnen:

- Fügen Sie die Apps optional einer App-Gruppe hinzu.

- Benutzer müssen Secure Work Space auf ihren Geräten einrichten, bevor sie zugewiesene gesicherte Apps installieren können.

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte**.
2. Suchen Sie nach einem Benutzerkonto.
3. Klicken Sie in den Suchergebnissen auf den Namen eines Benutzerkontos.
4. Klicken Sie im Abschnitt **Gruppen und Benutzern zugewiesene Apps** auf +.
5. Aktivieren Sie die Kontrollkästchen neben den Apps oder der App-Gruppe, die Sie dem Benutzerkonto zuweisen möchten.
6. Klicken Sie auf **Weiter**.
7. Führen Sie in der Dropdown-Liste **Verfügbarkeit** der App eine der folgenden Aktionen aus:
   - Damit Benutzer die App installieren müssen, wählen Sie **Erforderlich** aus.
   - Um zuzulassen, dass Benutzer die Anwendung installieren und entfernen, wählen Sie **Optional**.

     Hinweis: Wenn eine App gleichzeitig einem Benutzerkonto, der Benutzergruppe dieses Benutzerkontos und einer Gerätegruppe zugewiesen ist, wird die Verfügbarkeit der App, die der Gerätegruppe zugewiesen ist, vorrangig behandelt.

8. Wenn Sie Per App VPN-Einstellungen zu einer App zuweisen möchten, wählen Sie in der Dropdown-Liste **Per App VPN** die Einstellungen aus, die mit der App verknüpft werden sollen.
9. Führen Sie beim Hinzufügen einer iOS-App eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Wenn Sie kein VPP-Konto hinzugefügt haben oder keine iOS-App hinzufügen	1. Klicken Sie auf **Zuweisen**.
Wenn Sie eine iOS-App hinzufügen und mindestens ein VPP-Konto hinzugefügt haben	1. Klicken Sie auf **Weiter**. 2. Wählen Sie **Ja**, wenn Sie der iOS-App eine Lizenz hinzufügen möchten. Wählen Sie **Nein**, wenn Sie keine Lizenz zuweisen möchten oder keine Lizenz haben, die Sie der App zuweisen könnten. 3. Wenn Sie der App eine Lizenz zugewiesen haben, wählen Sie in der Dropdown-Liste **App-Lizenz erteilen** das VPP-Konto aus, das mit der App verknüpft werden soll. 4. Klicken Sie auf **Zuweisen**. Benutzer müssen sich entsprechend der Anweisungen im VPP Ihrer Organisation auf ihrem Gerät registrieren, bevor sie vorausbezahlte Apps

Aufgabe	Schritte
	installieren können. Benutzer müssen diese Aufgabe ein Mal erledigen. **Hinweis:** Wenn Sie mehr Lizenzen gewähren möchten, als verfügbar sind, kann der erste Benutzer, der auf die verfügbaren Lizenzen zugreift, die App installieren.

Verwandte Informationen
App-Verhalten auf Android-Geräten, auf Seite 160
App-Verhalten auf iOS-Geräten, auf Seite 166
App-Verhalten auf BlackBerry-Geräten, auf Seite 168

Ändern der einem Benutzer zugewiesenen Per App VPN-Einstellungen

Sie können die mit einer App oder einer App-Gruppe verknüpften VPN-Einstellungen für iOS-Geräte ändern, nachdem Sie die App oder App-Gruppe dem Benutzer oder der Benutzergruppe zugewiesen haben.

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte**.
2. Wenn die zu ändernden Per App VPN-Einstellungen einem Benutzerkonto zugewiesen sind, klicken Sie in den Sucherergebnissen auf den Namen eines Benutzerkontos.
3. Klicken Sie im Abschnitt **Gruppen und Benutzern zugewiesene Apps** auf die zu ändernden Per App VPN-Einstellungen.
4. Klicken Sie im Dialogfeld **Bearbeiten der Funktion „Per App VPN“** auf die Dropdownliste **Per App VPN**, und wählen Sie die Einstellungen in der Dropdown-Liste aus.
5. Klicken Sie auf **Speichern**.

Zuweisen einer BlackBerry OS-IT-Richtlinie, eines Profils oder einer Softwarekonfiguration zu einem Benutzerkonto

Bevor Sie beginnen:

- Vergewissern Sie sich, dass Sie die BlackBerry OS-Geräteaktivierung für das Benutzerkonto aktiviert haben.
- Erstellen Sie eine BlackBerry OS-IT-Richtlinie.
- Erstellen Sie eine Softwarekonfiguration.
- Erstellen Sie ein Wi-Fi- oder VPN-Profil für BlackBerry OS-Geräte. Weitere Informationen finden Sie im Handbuch für Administratoren unter help.blackberry.com/detectLang/bes5.
- Erstellen Sie eine Push- oder Pull-Zugriffssteuerungsregel für BlackBerry OS-Geräte. Weitere Informationen finden Sie im Handbuch für Administratoren unter help.blackberry.com/detectLang/bes5.

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte**.
2. Suchen Sie nach einem Benutzerkonto.
3. Klicken Sie in den Suchergebnissen auf den Namen eines Benutzerkontos.
4. Klicken Sie auf dem Register **Benutzerzusammenfassung** im Abschnitt **IT-Richtlinie, Profile und Softwarekonfigurationen** auf +.
5. Klicken Sie auf **IT-Richtlinie**, **Wi-Fi**, **VPN**, **Push einer Zugriffssteuerungsregel**, **Pull einer Zugriffssteuerungsregel** oder **Softwarekonfiguration**.
6. Klicken Sie in der Dropdown-Liste auf den Namen der IT-Richtlinie, des Profils, der Zugriffssteuerungsregel oder der Softwarekonfiguration, die bzw. das Sie dem Benutzer zuweisen möchten.
7. Klicken Sie auf **Zuweisen**.

Verwandte Informationen

Zuweisen von BlackBerry OS-IT-Richtlinien und Auflösen von Konflikten zwischen IT-Richtlinien, auf Seite 146

Anzeigen der aufgelösten BlackBerry OS-IT-Richtlinienregeln, die einem Benutzerkonto zugewiesen sind

Wenn ein Benutzer Mitglied von mehreren Benutzergruppen mit unterschiedlichen BlackBerry OS-IT-Richtlinien ist, bereinigt BES12 die widersprüchlichen IT-Richtlinien oder die IT-Richtlinieneinstellungen mithilfe des Schlichtungsverfahrens, das Sie in den BlackBerry OS-Einstellungen festgelegt haben. Sie können die Ergebnisse der BlackBerry OS-IT-Richtlinienschlichtung und die bereinigten Einstellungen zu jeder Bestimmung unter „Erweiterte Einstellungen“ auf der Registerkarte „Benutzerzusammenfassung“ anzeigen. Wenn eine IT-Richtlinienregel mit den verschiedenen BlackBerry OS-IT-Richtlinien übereinstimmt, die auf das Benutzerkonto angewendet wurden, wird diese Regel nicht unter den IT-Richtlinien angezeigt.

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte**.
2. Suchen Sie nach einem Benutzerkonto.
3. Klicken Sie in den Suchergebnissen auf den Namen eines Benutzerkontos.
4. Klicken Sie auf dem Register **Benutzerzusammenfassung** im Abschnitt **IT-Richtlinie, Profile und Softwarekonfigurationen** auf **Erweiterte Einstellungen**.
5. Klicken Sie auf die Registerkarte **Richtlinien**.
6. Klicken Sie im Abschnitt **Aufgelöste IT-Richtliniennamen** auf den Namen der BlackBerry OS-IT-Richtlinie.

Verwenden von Filtern zum Anpassen der Benutzer- und Geräteansicht

Sie können Filter verwenden, um nur die Benutzer und Informationen anzuzeigen, die für Ihre Aufgabe relevant sind. Sie können beispielsweise Benutzer nach Gruppenmitgliedschaft, zugewiesenen Richtlinien, Kompatibilitätsstatus, OS-Familie und -Version, Hardwarelieferant, Dienstanbieter und Roaming-Status filtern und anzeigen. Sie können die Liste filtern, indem Sie

jeweils einen Filter oder mehrere Filter gleichzeitig auswählen. Beim Auswählen von Filtern werden Filter, die keine Ergebnisse anzeigen würden, automatisch in den jeweiligen Kategorien ausgelassen.

Wenn Sie die Mehrfachauswahl ausschalten, wird der jeweilige Filter bei Auswahl angewendet, und Sie können jeweils nur einen Filter für eine Kategorie auswählen.

Wenn Sie die Mehrfachauswahl einschalten, können Sie mehrere Filter auswählen, bevor Sie diese anwenden, und Sie können für jede Kategorie mehrere Filter auswählen.

Zu weiteren Analyse- und Reporting-Zwecken können Sie die Liste von Benutzern in eine .csv-Datei exportieren.

Filtern von Benutzern und Geräten

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte**.
2. Klicken Sie im linken Fensterbereich auf , um die Mehrfachauswahl ein- oder auszuschalten.
3. Klicken Sie unter **Filter** auf eine Kategorie, um diese zu erweitern.
4. Wählen Sie die Filter aus, die Sie anwenden möchten. Neben jedem Filter können Sie die Anzahl der Ergebnisse sehen, wenn Sie den betreffenden Filter anwenden.
5. Wenn Sie die Mehrfachauswahl aktiviert haben, klicken Sie auf **Senden**.
6. Optional führen Sie einen der folgenden Schritte aus:
    - Um weitere Filter anzuwenden, wiederholen Sie im linken Fensterbereich die Schritte 3 bis 5.
    - Zum Entfernen von Filtern klicken Sie im rechten Fensterbereich auf × neben dem Filter, den Sie entfernen möchten.
    - Zum Entfernen aller Filter klicken Sie im rechten Fensterbereich auf **Alle entfernen**.

Exportieren einer Benutzerliste in eine .csv-Datei

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte**.
2. Filtern Sie im linken Fensterbereich die Details, die in den Bericht aufgenommen werden sollen.
3. In der gefilterten Liste wählen Sie die Benutzer aus, die in den Bericht aufgenommen werden sollen.
4. Klicken Sie auf , und speichern Sie die Datei.

Verwalten von Gerätegruppen

23

Sie können Gerätegruppen für die effiziente Verwaltung ähnlicher Geräte definieren und erstellen.

Schritte zum Erstellen und Verwalten von Gerätegruppen

Wenn Sie Gerätegruppen erstellen und verwalten, führen Sie die folgenden Aktionen aus:

Schritt	Aktion
1	Optional: Wählen Sie Benutzergruppen aus, auf die die Abfrage beschränkt werden soll.
2	Erstellen Sie eine Abfrage, um einen bestimmten Satz an Geräten zu spezifizieren.
3	Weisen Sie den in der Abfrage definierten Geräten IT-Richtlinien, Profile und Apps zu.

Erstellen einer Gerätegruppe

Eine Gerätegruppe ist eine Gruppe von Geräten mit gemeinsamen Attributen, wie zum Beispiel Modell und Hersteller, Betriebssystem und Version, Dienstanbieter und inwieweit das Gerät Eigentum der Organisation oder des Benutzers ist.Auf der Grundlage der von Ihnen definierten Geräteattribute verschiebt BES12 die Geräte automatisch in eine Gerätegruppe bzw. entfernt sie daraus.

Sie können die Gerätegruppen dazu nutzen, um den Geräten, die einem einzelnen Benutzer zugewiesen sind, verschiedene Richtlinien, Profile und Apps zuzuweisen. Sie können beispielsweise eine Gerätegruppe verwenden, um eine bestimmte IT-Richtlinie für alle Geräte anzuwenden, auf denen BlackBerry 10 OS ausgeführt wird, oder für alle HTC EVO-Geräte, auf denen Android OS 4.0 oder höher im T-Mobile-Netzwerk im Einsatz ist.

Richtlinien, Profile und Apps, die einer Gerätegruppe zugewiesen wurden, haben Priorität vor denen, die einem Benutzer oder einer Benutzergruppe zugewiesen wurden. Sie können den Gerätegruppen jedoch keine Aktivierungsprofile oder Benutzerzertifikate zuweisen.

Gerätegruppen gelten nicht für Geräte mit BlackBerry OS (Version 5.0 bis 7.1). Selbst wenn Sie eine Gerätegruppenabfrage erstellen, zu der unter logischen Aspekten auch Ihre BlackBerry OS-Geräte gehören müssten, sind sie in der Gerätegruppe nicht enthalten.

Erstellen einer Gerätegruppe

1. Klicken Sie in der Menüleiste auf **Gruppen**.
2. Klicken Sie auf die Registerkarte **Gerätegruppen**.
3. Klicken Sie auf .
4. Geben Sie einen Namen für die Gerätegruppe ein.
5. Im Abschnitt **Beschränken auf Benutzergruppen** können Sie eine oder mehrere Benutzergruppen auswählen, für die die Gerätegruppe angewandt wird. Wenn Sie keine Benutzergruppen auswählen, wird die Gerätegruppe für alle aktivierten Geräte angewandt.
6. Klicken Sie in der ersten Dropdown-Liste im Abschnitt **Geräteabfrage** auf die Option **Beliebige** oder **Alle**.

   Wenn Sie die Option **Alle** auswählen, müssen auf die Geräte alle von Ihnen definierten Attribute zutreffen, um der Gerätegruppe anzugehören. Wenn Sie die Option **Beliebige** auswählen, müssen auf die Geräte nur die von Ihnen definierten Attribute zutreffen, um der Gerätegruppe anzugehören.
7. Führen Sie im Feld **Geräteabfrage** eine der folgenden Aktionen aus:
   - Klicken Sie in der Dropdown-Liste **Attribut** auf ein Attribut.
   - Klicken Sie in der Dropdown-Liste **Betreiber** auf einen Betreiber.
   - Klicken Sie in der Dropdown-Liste **Wert** auf einen Wert, oder geben Sie einen ein.

   Sie können Ihre Abfrage bearbeiten, indem Sie Zeilen hinzufügen oder entfernen.
8. Klicken Sie auf **Weiter**.
9. Um der Gerätegruppe eine IT-Richtlinie oder ein Profil zuzuweisen, führen Sie die folgenden Aktionen aus:
   a. Klicken Sie im Abschnitt **IT-Richtlinien und -Profile** auf +.
   b. Klicken Sie auf **IT-Richtlinie** oder auf einen Profiltyp.
   c. Klicken Sie in der Dropdown-Liste auf den Namen der IT-Richtlinie oder des Profils, die bzw. das Sie der Gruppe zuweisen möchten.
   d. Klicken Sie auf **Zuweisen**.
10. Wenn Sie der Gerätegruppe eine App zuweisen möchten, klicken Sie im Abschnitt **Zugewiesene Apps** auf +.
11. Suchen Sie nach der App.
12. Wählen Sie in den Suchergebnissen die App aus.
13. Klicken Sie auf **Weiter**.
14. Führen Sie in der Dropdown-Liste **Verfügbarkeit** der App eine der folgenden Aktionen aus:
    - Wenn es sich bei der App um eine iOS- oder Android-App handelt: Wenn Benutzer die Aktionen ausführen müssen, die für Apps in dem Kompatibilitätsprofil definiert wurden, das dem entsprechenden Benutzer zugewiesen wurde, wählen Sie **Erforderlich**.

- Wenn es sich bei der App um eine Windows Phone-App handelt: Damit auf den zugewiesenen Geräten automatisch eine interne App installiert wird, wählen Sie **Erforderlich** aus. Wenn Benutzer die erforderliche interne App deinstallieren, müssen sie die folgenden Aktionen ausführen, die in dem ihnen zugewiesenen Kompatibilitätsprofil definiert wurden. Wählen Sie bei Apps, die über den Windows Phone Store hinzugefügt wurden, die Option **Erforderlich** aus. Mit dieser Einstellung müssen die Benutzer die Aktionen befolgen, die für Apps in dem ihnen zugewiesenen Kompatibilitätsprofil definiert wurden. Dies gilt nur für Geräte mit Windows Phone 8.1 oder höher.
- Wenn es sich bei der App um eine interne BlackBerry 10-App handelt: Um die interne App automatisch auf zugewiesenen Geräten zu installieren, wählen Sie **Erforderlich**. Diese Option ist nur für interne BlackBerry 10-Apps verfügbar. Apps, die über die BlackBerry World-Verkaufsplattform hinzugefügt werden, können nur optional sein.
- Um Benutzern das Installieren und Entfernen der App zu gestatten, wählen Sie **Optional**.

  Hinweis: Dieselbe App kann entweder direkt einem Benutzerkonto zugewiesen werden, oder sie kann von einer Benutzergruppe oder Gerätegruppe geerbt werden. Die Einstellungen der App (ob sie beispielsweise erforderlich ist), werden entsprechend der Priorität zugewiesen: Gerätegruppen haben Vorrang vor Benutzerkonten und Benutzergruppen.

15. Klicken Sie auf **Zuweisen**.
16. Führen Sie für eine zugewiesene App – falls erforderlich – eine der folgenden Aktionen aus.
    - Klicken Sie den App-Namen, um die Details der App anzuzeigen.
    - So ändern Sie die **Verfügbarkeit** für eine App:
      1. Klicken Sie auf die Verfügbarkeit der App.
      2. Wählen Sie eine neue Verfügbarkeit aus.
      3. Klicken Sie auf **Speichern**.
    - Um eine zugewiesene App zu entfernen, klicken Sie neben der App auf ×.
17. Wenn Sie die Eigenschaften der Gerätegruppe festgelegt haben, klicken Sie auf **Speichern**.

Festlegen von Parametern für Gerätegruppen

Konfigurieren Sie beim Erstellen einer Gerätegruppe eine Geräteabfrage mit mindestens einer Attributeingabe. Sie können festlegen, ob ein Gerät zur Gerätegruppe gehört, wenn nur eine Attributeingabe übereinstimmt, oder ob dazu alle Attributeingaben übereinstimmen müssen. Jede Attributeingabe enthält ein Attribut, einen Operator und einen Wert. Die nachfolgende Tabelle beschreibt die einzelnen Elemente.

Attribut	Operatoren	Werte
Betreiber	• =	Textfeld. Geben Sie den Namen eines Dienstanbieter ein, z. B. T-Mobile oder Bell.

Attribut	Operatoren	Werte
	• != • Beginnt mit	
Hersteller	• = • != • Beginnt mit	Textfeld. Geben Sie den Namen eines Geräteherstellers ein, z. B. Apple oder BlackBerry.
Modell	• = • != • Beginnt mit	Textfeld. Geben Sie den Namen eines Gerätemodells ein, z. B. iPhone oder BlackBerry Q10.
Betriebssystem	• = • !=	Dropdown-Liste. Wählen Sie Android, BlackBerry 10, iOS oder Windows Phone aus.
Betriebssystemversion	• = • != • >= • <=	Textfeld. Geben Sie eine Version des Betriebssystems ein, z. B. 7.1.1 oder 10.3. Wenn Sie dieses Attribut verwenden, müssen Sie auch das Betriebssystemattribut festlegen, um Überschneidungen mit Betriebssystemversionen zu vermeiden.
Eigentum	• = • !=	Dropdown-Liste. Wählen Sie „Geschäftlich“, „Privat“ oder „Nicht angegeben“ aus.

Anzeigen einer Gerätegruppe

1. Klicken Sie in der Menüleiste auf **Gruppen**.
2. Klicken Sie auf die Registerkarte **Gerätegruppen**.
3. Suchen Sie die Gerätegruppe, die Sie anzeigen möchten.
4. Klicken Sie auf die Gerätegruppe.
5. Führen Sie eine der folgenden Aktionen aus:
    - Klicken Sie auf die Registerkarte **Geräte**, um die Geräte anzuzeigen, die der Gerätegruppe zugewiesen wurden.
    - Wählen Sie die Registerkarte **Einstellungen**, um die Benutzergruppen, Geräteabfragen, IT-Richtlinien, Profile oder Apps anzuzeigen, die der Gerätegruppe zugewiesen wurden.

Klicken Sie auf den Namen einer Gerätegruppe.

1. Klicken Sie in der Menüleiste auf **Gruppen**.
2. Klicken Sie auf die Registerkarte **Gerätegruppen**.
3. Suchen Sie die Gerätegruppe, die Sie anzeigen möchten.
4. Klicken Sie auf die Gerätegruppe.
5. Klicken Sie auf .
6. Ändern Sie den Namen der Gerätegruppe.
7. Klicken Sie auf **Weiter**.
8. Klicken Sie auf **Speichern**.

Löschen einer Gerätegruppe

1. Klicken Sie in der Menüleiste auf **Gruppen**.
2. Klicken Sie auf die Registerkarte **Gerätegruppen**.
3. Suchen Sie die Gerätegruppe, die Sie anzeigen möchten.
4. Klicken Sie auf die Gerätegruppe.
5. Klicken Sie auf .
6. Klicken Sie auf **Löschen**.

Aktivieren von beim DEP registrierten iOS-Geräten

24

Sie können iOS-Geräte beim Programm zur Geräteregistrierung (DEP) von Apple registrieren und diesen mit der BES12-Verwaltungskonsole Registrierungskonfigurationen zuweisen. Registrierungskonfigurationen enthalten zusätzliche Regeln, etwa „Beaufsichtigten Modus aktivieren“, die den Geräten bei der MDM-Registrierung zugewiesen werden.

Wenn die Geräte aktiviert werden, sendet BES12 Richtlinien und Profile, die Sie Benutzern zugewiesen haben.

Wenn Sie ein Gerät für die Verwendung von Secure Work Space konfigurieren oder einem Benutzer ein Kompatibilitätsprofil zuweisen, muss der Benutzer nach der Geräteaktivierung den BES12 Client starten.

Voraussetzung: Verwendung des BES12 Client für beim DEP registrierte Geräte

- Fügen Sie den BES12 Client der App-Liste hinzu. Der BES12 Client steht im App Store zur Verfügung.
- Weisen Sie den BES12 Client Benutzerkonten oder -gruppen zu.

Weitere Informationen finden Sie in der Dokumentation für Administratoren unter „Verwalten von Apps auf Geräten“.

Schritte zum Aktivieren von Geräten, die beim DEP registriert sind

Wenn Sie iOS-Geräte aktivieren, die beim Programm zur Geräteregistrierung von Apple (DEP) registriert sind, führen Sie die folgenden Aktionen aus:

Schritt	Aktion
1	Registrieren Sie die Geräte beim Programm zur Geräteregistrierung und weisen Sie sie einem MDM-Server zu.
2	Weisen Sie den Geräten eine Registrierungskonfiguration zu.

Registrieren von iOS-Geräten beim DEP und Zuweisen eines MDM-Servers

Zum Registrieren von Geräten beim Programm zur Geräteregistrierung (DEP) müssen Sie die Geräteseriennummern auf dem Apple DEP-Portal eingeben und die Geräte einem MDM-Server zuweisen. Sie können die Seriennummern verschiedene Weise eingeben:

- Eintippen der einzelnen Nummern
- Auswählen der Bestellnummern, die den Geräten beim Kauf von Apple zugewiesen wurde
- Hochladen einer CSV-Datei mit den Seriennummern

Bevor Sie beginnen: Konfigurieren Sie BES12 für die Verwendung von DEP, bevor Sie iOS-Geräte registrieren. Weitere Informationen zum Konfigurieren von BES12 finden Sie in der Dokumentation zur Konfiguration.

1. Geben Sie im Browser **deploy.apple.com** ein.
2. Melden Sie sich bei Ihrem DEP-Konto an.
3. Klicken Sie auf **Geräte verwalten**.
4. Folgen Sie den Anweisungen zum Eingeben der Geräteseriennummern.
5. Weisen Sie die Seriennummern einem MDM-Server zu.

Wenn Sie fertig sind: Weisen Sie den Geräten in der BES12-Verwaltungskonsole Registrierungskonfigurationen zu.

Zuweisen von Registrierungskonfigurationen zu iOS-Geräten

Wenn Sie eine Registrierungskonfiguration erstellt und „Alle neuen Geräte automatisch dieser Konfiguration zuweisen“ ausgewählt haben, weist BES12 die Konfiguration automatisch Geräten zu, wenn Sie diese beim DEP registrieren. Wenn BES12 Registrierungskonfigurationen nicht automatisch zuweist, müssen Sie dies tun.

Bevor Sie beginnen: Registrieren Sie die iOS-Geräte beim DEP, und weisen Sie ihnen einen MDM-Server zu.

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte** > **Apple DEP-Geräte**.
2. Aktivieren Sie die Kontrollkästchen neben den Geräten, denen Sie eine Registrierungskonfiguration zuweisen möchten.
3. Klicken Sie auf .
4. Klicken Sie in der Dropdown-Liste **Registrierungskonfiguration** auf die Registrierungskonfiguration, die Sie zuweisen möchten.
5. Klicken Sie auf **Zuweisen**.

Wenn Sie fertig sind: Verteilen Sie die iOS-Geräte an die Benutzer zur Aktivierung.

Entfernen einer iOS-Geräten zugewiesenen Registrierungskonfiguration

Wenn Sie Geräten eine Registrierungskonfiguration zugewiesen haben, diese jedoch noch nicht auf die Geräte angewendet wurde, können Sie die Registrierungskonfiguration von den Geräten entfernen.

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte** > **Apple DEP-Geräte**.
2. Aktivieren Sie die Kontrollkästchen neben den Geräten, von denen Sie eine Registrierungskonfiguration entfernen möchten.
3. Klicken Sie auf .
4. Klicken Sie auf **Entfernen**.

Wenn Sie fertig sind: Weisen Sie den Geräten eine Registrierungskonfiguration zu.

Verwalten von Registrierungskonfigurationen

Wenn Sie BES12 für die Verwendung des Registrierungsprogramms (DEP) von Apple konfigurieren, müssen Sie eine Registrierungskonfiguration erstellen. Sie können weitere Registrierungskonfigurationen hinzufügen, Registrierungskonfigurationen entfernen und ihre Einstellungen ändern.

Informationen zum Konfigurieren von BES12 für die Verwendung von DEP finden Sie in der Dokumentation zur Konfiguration.

Hinzufügen einer Registrierungskonfiguration

Sie können nach Bedarf beliebig viele Registrierungskonfiguration erstellen.

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Klicken Sie im linken Fensterbereich auf **Externe Integration** > **Programm zur Geräteregistrierung von Apple**.
3. Klicken Sie im Abschnitt **DEP-Anmeldungskonfigurationen** auf +.
4. Füllen Sie die Felder aus, und aktivieren Sie die Kontrollkästchen für die Elemente, die Ihre Registrierungskonfiguration enthalten soll.
    - Die Einstellung „Alle neuen Geräte automatisch dieser Konfiguration zuweisen“ kann nur für eine Registrierungskonfiguration aktiviert werden. Wenn Sie beispielsweise eine Registrierungskonfiguration unter dem Namen „Konfiguration_2“ mit dieser Einstellung erstellen und es bereits eine Registrierungskonfiguration „Konfiguration_1“ mit dieser Einstellung gibt, löscht BES12 die Einstellung für Konfiguration_1.
    - Wenn Sie die Option „Alle neuen Geräte automatisch dieser Konfiguration zuweisen“ auswählen, weist BES12 die Registrierungskonfiguration neu beim DEP von Apple registrierten iOS-Geräten automatisch zu.

- Wenn Sie zuvor eine Registrierungskonfiguration mit der Einstellung „Alle neuen Geräte automatisch dieser Konfiguration zuweisen“ erstellt haben und diese auf Geräte angewendet wurde, weist BES12 die neue Registrierungskonfiguration den Geräten nicht zu.
- Wenn Sie eine neue Registrierungskonfiguration Geräten zuweisen möchten, und deren Aktivierung noch aussteht, können Sie die zuvor zugewiesene Registrierungskonfiguration entfernen und den Geräten die neue Registrierungskonfiguration zuweisen.
- Wenn Sie im Bereich „Gerätekonfiguration“ weder „Beaufsichtigten Modus aktivieren“ noch „Entfernen des MDM-Profils zulassen“ auswählen, werden Sie von BES12 beim Speichern der Registrierungskonfiguration zur Auswahl eines dieser Elemente aufgefordert. Sie müssen mindestens eines dieser Elemente auswählen. Optional können Sie beide Elemente auswählen.

5. Klicken Sie auf **Speichern**.
6. Wenn Sie die Option „Alle neuen Geräte automatisch dieser Konfiguration zuweisen“ ausgewählt haben, klicken Sie auf **Ja**.

Wenn Sie fertig sind: Weisen Sie die Registrierungskonfiguration Geräten zu.

Entfernen einer zugewiesenen Registrierungskonfiguration

Wenn Sie eine Registrierungskonfiguration, die Geräten zugewiesen wurde, vor der Anwendung der Registrierungskonfiguration entfernen, entfernt BES12 die Registrierungskonfiguration von den Gerätedatensätzen.

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Klicken Sie im linken Fensterbereich auf **Externe Integration** > **Programm zur Geräteregistrierung von Apple**.
3. Klicken Sie im Abschnitt **DEP-Anmeldungskonfigurationen** auf ×.
4. Klicken Sie auf **Ja**.

Wenn Sie fertig sind: Wenn BES12 die Registrierungskonfiguration von Geräten entfernt, weisen Sie diesen eine Registrierungskonfiguration zu.

Ändern der Einstellungen einer Registrierungskonfiguration

Wenn Sie Geräten eine Registrierungskonfiguration zugewiesen haben und diese noch nicht auf die Geräte angewendet wurde, aktualisiert BES12 die Registrierungskonfiguration, wenn Sie die Änderungen an der Registrierungskonfiguration speichern.

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Klicken Sie im linken Fensterbereich auf **Externe Integration** > **Programm zur Geräteregistrierung von Apple**.
3. Klicken Sie im Bereich **DEP-Anmeldungskonfigurationen** auf den Namen der Konfiguration, die Sie ändern möchten.
4. Ändern Sie die Einstellungen.
5. Klicken Sie auf **Speichern**.

Anzeigen der Einstellungen einer zugewiesenen Registrierungskonfiguration

Wenn eine Registrierungskonfiguration einem iOS-Gerät zugewiesen und noch ausstehend ist, können Sie die Einstellungen der Registrierungskonfiguration anzeigen.

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte** > **Apple DEP-Geräte**.
2. Klicken Sie in der Spalte **Registrierungskonfiguration** auf den Namen einer Registrierungskonfiguration.

Anzeigen der Benutzerdetails für ein aktiviertes Gerät

Nachdem ein Gerät aktiviert wurde, können Sie Details zu dessen Benutzer, beispielsweise die Gruppen, denen er zugewiesen ist, anzeigen.

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte** > **Apple DEP-Geräte**.
2. Klicken Sie in der Spalte **Anzeigename** auf den Namen eines Benutzers.

Aktivieren von Geräten

25

Wenn Sie ein Gerät aktivieren, verknüpfen Sie das Gerät mit BES12, damit Sie die Geräte verwalten und die Benutzer auf ihren Geräten auf Geschäftsdaten zugreifen können.

Wenn ein Gerät aktiviert wurde, können Sie IT-Richtlinien und Profile versenden, um die verfügbaren Funktionen zu überwachen und die Sicherheit der geschäftlichen Daten sicherzustellen. Sie können auch Apps zuweisen, die der Benutzer installieren kann. Je nachdem, wie viel Kontrolle die ausgewählte Aktivierungsart zulässt, können Sie auch das Gerät schützen, indem Sie den Zugriff auf bestimmte Daten einschränken, dezentral Kennwörter festlegen, das Gerät sperren oder Daten löschen.

Sie können die Aktivierungsarten so zuweisen, dass die besonderen Anforderungen je nachdem, ob die Geräte Ihrer Organisation oder den Benutzern gehören, individuell umgesetzt werden. Durch die verschiedenen Aktivierungsarten haben Sie einen unterschiedlich hohen Einfluss auf die geschäftlichen und privaten Daten auf den Geräten: von der kompletten Kontrolle aller Daten bis hin zur Beschränkung der Kontrolle auf die geschäftlichen Daten.

Schritte zur Aktivierung von Geräten

Beim Aktivieren von Geräten führen Sie die folgenden Aktionen aus:

Schritt	Aktion
1	Stellen Sie sicher, dass alle Aktivierungsvoraussetzungen erfüllt sind.
2	Konfigurieren Sie die standardmäßigen Aktivierungseinstellungen.
3	Wenn Sie Android for Work unterstützen möchten, führen Sie jegliche zusätzlichen Aufgaben aus.
4	Aktualisieren Sie die Vorlage für die Aktivierungs-E-Mail.
5	Erstellen Sie ein Aktivierungsprofil, und weisen Sie es einem Benutzerkonto oder einer Gruppe zu, der der Benutzer angehört.
6	Richten Sie ein Aktivierungskennwort für den Benutzer ein.

Voraussetzungen: Aktivierung

Für alle Geräte:

- Eine verfügbare Lizenz für die verwendete Aktivierungsart
- Eine aktive kabellose Verbindung

iOS- und Windows Phone-Geräte:

- BES12 Client auf dem Gerät installiert

Android-Geräte:

- BES12 Client auf dem Gerät installiert
    - Zur Unterstützung von Android for Work oder KNOX Workspace installieren Sie die die neueste Version von BES12 Client über Google Play vor dem Aktivieren des Geräts.
- Zur Unterstützung von Android for Work, Android OS 5.1 (Lollipop)
- Zur Unterstützung von KNOX MDM IT-Richtlinien, Samsung KNOX MDM 4.0 oder höher auf dem Gerät installiert
- Zur Unterstützung von KNOX Workspace, Samsung KNOX MDM 5.0 oder höher und Samsung KNOX 2.0 oder höher auf dem Gerät installiert

Für Geräte mit BlackBerry OS (Version 5.0 bis 7.1):

- Ein Benutzerkonto in einem Verzeichnis auf dem geschäftlichen Mailserver, mit dem der BlackBerry OS-Mailserver eine Verbindung herstellt
- BlackBerry OS-Geräteaktivierung für das Benutzerkonto aktiviert

Weitere Informationen zu Lizenzen finden Sie in der Dokumentation zur Lizenzierung.

Lizenzanforderungen für Aktivierungsarten

Die folgende Tabelle führt die erforderliche Lizenz für jede Aktivierungsart auf. BES12 prüft in der angegebenen Reihenfolge nach verfügbaren Lizenzen. Wenn Sie beispielsweise ein BlackBerry 10-Gerät mit der Aktivierungsart „Geschäftlich und persönlich – Unternehmen“ aktivieren und für BES12 Silver- und Gold-Serverlizenzen verfügbar sind, nutzt das Gerät eine Silver-Lizenz.

Welche Art von Lizenz ein Gerät nutzt können Sie in den Gerätedetails des Benutzers in der Verwaltungskonsole prüfen.

Hinweis: In den Lizenzinformationen der Geräteangaben wird Gold - Flex als erforderliche Lizenz für Samsung KNOX Workspace-Geräte angezeigt. Verfügt das Gerät nicht über die erforderliche SIM-Lizenz, verwendet es eine Gold - KNOX Workspace-Serverlizenz, sofern eine solche verfügbar ist, andernfalls eine Gold - Flex-Serverlizenz.

BlackBerry 10-Geräte

Aktivierungsart	Beschreibung	Erforderliche Lizenz
Geschäftlich und persönlich – Unternehmen	Die Geräte verfügen über einen persönlichen und einen geschäftlichen Bereich. Administratoren haben nur die Kontrolle über den geschäftlichen Bereich.	Eine der folgenden Bedingungen muss erfüllt sein: 1. Silver-SIM-Lizenz 2. Gold-SIM-Lizenz 3. Silver-Serverlizenz 4. Gold-Serverlizenz 5. Gold - Flex-Serverlizenz
Geschäftlich und persönlich – Reguliert	Die Geräte verfügen über einen persönlichen und einen geschäftlichen Bereich. Administratoren haben die Kontrolle über beide Bereiche.	Eine der folgenden Bedingungen muss erfüllt sein: 1. Gold-SIM-Lizenz 2. Gold-Serverlizenz 3. Gold - Flex-Serverlizenz
Nur geschäftlicher Bereich	Die Geräte verfügen nur über einen geschäftlichen Bereich. Administratoren haben die volle Kontrolle über die Geräte.	Eine der folgenden Bedingungen muss erfüllt sein: 1. Gold-SIM-Lizenz 2. Gold-Serverlizenz 3. Gold - Flex-Serverlizenz

iOS-Geräte

Aktivierungsart	Beschreibung	Erforderliche Lizenz
MDM-Steuerelemente	Es wird kein separater geschäftlicher Bereich auf den Geräten erstellt. Administratoren stehen einfache Verwaltungsmöglichkeiten über iOS-eigene Optionen zur Verfügung.	Eine der folgenden Bedingungen muss erfüllt sein: 1. Silver-SIM-Lizenz 2. Gold-SIM-Lizenz 3. Silver-Serverlizenz 4. Gold - Secure Work Space-Serverlizenz 5. Gold-Serverlizenz 6. Gold - Flex-Serverlizenz

Aktivierungsart	Beschreibung	Erforderliche Lizenz
Geschäftlich und persönlich – vollständige Kontrolle	Es wird ein separater geschäftlicher Bereich auf den Geräten erstellt. Administratoren haben die volle Kontrolle über die Geräte.	Eine der folgenden Bedingungen muss erfüllt sein: 1. Gold-SIM-Lizenz 2. Gold - Secure Work Space-Serverlizenz
Geschäftlich und persönlich – Benutzer-Datenschutz	Es wird ein separater geschäftlicher Bereich auf den Geräten erstellt. Administratoren haben nur die Kontrolle über den geschäftlichen Bereich.	Eine der folgenden Bedingungen muss erfüllt sein: 1. Gold-SIM-Lizenz 2. Gold - Secure Work Space-Serverlizenz

Windows Phone-Geräte

Aktivierungsart	Beschreibung	Erforderliche Lizenz
MDM-Steuerelemente	Es wird kein separater geschäftlicher Bereich auf den Geräten erstellt. Administratoren stehen einfache Verwaltungsmöglichkeiten über Windows Phone OS-eigene Optionen zur Verfügung.	Eine der folgenden Bedingungen muss erfüllt sein: 1. Silver-SIM-Lizenz 2. Gold-SIM-Lizenz 3. Silver-Serverlizenz 4. Gold - Secure Work Space-Serverlizenz 5. Gold-Serverlizenz 6. Gold - Flex-Serverlizenz

Android-Geräte

Aktivierungsart	Beschreibung	Erforderliche Lizenz
MDM-Steuerelemente	Es wird kein separater geschäftlicher Bereich auf den Geräten erstellt. Administratoren stehen einfache Verwaltungsmöglichkeiten über Android OS-eigene Optionen oder Optionen von Samsung KNOX zur Verfügung. Diese Aktivierungsart gilt für: • Android-Geräte, die Android MDM unterstützen	Eine der folgenden Bedingungen muss erfüllt sein: 1. Silver-SIM-Lizenz 2. Gold-SIM-Lizenz 3. Silver-Serverlizenz 4. Gold - Secure Work Space-Serverlizenz 5. Gold-Serverlizenz

Aktivierungsart	Beschreibung	Erforderliche Lizenz
	• Samsung-Geräte, die KNOX MDM unterstützen	6. Gold - KNOX Workspace-Serverlizenz (nur Samsung KNOX MDM-Geräte) 7. Gold - Flex-Serverlizenz
Geschäftlich und persönlich – vollständige Kontrolle (Secure Work Space)	Es wird ein separater geschäftlicher Bereich auf den Geräten erstellt. Administratoren haben die volle Kontrolle über die Geräte. Diese Aktivierungsart gilt für: • Android-Geräte, die Android MDM unterstützen • Samsung-Geräte, die KNOX MDM unterstützen	Eine der folgenden Bedingungen muss erfüllt sein: 1. Gold-SIM-Lizenz 2. Gold - Secure Work Space-Serverlizenz
Geschäftlich und persönlich – Benutzer-Datenschutz (Secure Work Space)	Es wird ein separater geschäftlicher Bereich auf den Geräten erstellt. Administratoren haben nur die Kontrolle über den geschäftlichen Bereich. Diese Aktivierungsart gilt für: • Android-Geräte, die Android MDM unterstützen	Eine der folgenden Bedingungen muss erfüllt sein: 1. Gold-SIM-Lizenz 2. Gold - Secure Work Space-Serverlizenz
Geschäftlich und persönlich – vollständige Kontrolle (Samsung KNOX)	Es wird ein separater geschäftlicher Bereich auf den Geräten erstellt. Administratoren haben die volle Kontrolle über die Geräte. Diese Aktivierungsart gilt für: • Samsung-Geräte, die KNOX Workspace unterstützen	Eine der folgenden Bedingungen muss erfüllt sein: 1. Gold-SIM-Lizenz 2. Gold - KNOX Workspace-Serverlizenz 3. Gold - Flex-Serverlizenz
Nur geschäftlicher Bereich (Samsung KNOX)	Die Geräte verfügen nur über einen geschäftlichen Bereich. Administratoren haben die volle Kontrolle über die Geräte. Diese Aktivierungsart gilt für: • Samsung-Geräte, die KNOX Workspace unterstützen	Eine der folgenden Bedingungen muss erfüllt sein: 1. Gold-SIM-Lizenz 2. Gold - KNOX Workspace-Serverlizenz 3. Gold - Flex-Serverlizenz

Aktivierungsart	Beschreibung	Erforderliche Lizenz
Geschäftlich und persönlich – Benutzer-Datenschutz (Android for Work)	Es wird ein separates geschäftliches Profil auf den Geräten erstellt. Administratoren haben nur die Kontrolle über das geschäftliche Profil. Diese Aktivierungsart gilt für: • Android-Geräte, die Android for Work unterstützen	Eine der folgenden Bedingungen muss erfüllt sein: 1. Silver-SIM-Lizenz 2. Gold-SIM-Lizenz 3. Silver-Serverlizenz 4. Gold - Secure Work Space-Serverlizenz 5. Gold-Serverlizenz 6. Gold - Flex-Serverlizenz
Geschäftlich und persönlich – Benutzer-Datenschutz (Android for Work - Premium)	Es wird ein separates geschäftliches Profil auf den Geräten erstellt. Administratoren haben nur die Kontrolle über das geschäftliche Profil. Diese Aktivierungsart gilt für: • Android-Geräte, die Android for Work unterstützen Diese Aktivierungsart ist zur Verwendung von BlackBerry Secure Connect Plus auf Android for Work-Geräten erforderlich.	Eine der folgenden Bedingungen muss erfüllt sein: 1. Gold-SIM-Lizenz 2. Gold-Serverlizenz 3. Gold - Flex-Serverlizenz

Verwalten des Standardablaufs und der Länge des Aktivierungskennworts

Sie können die Standardzeit festlegen, die ein Aktivierungskennwort gültig bleiben soll, bevor es abläuft. Sie können auch die Kennwortlänge für das automatisch generierte Kennwort bestimmen, das in einer der Aktivierungs-E-Mail-Nachrichten an die Benutzer gesendet wird. Außerdem können Sie festlegen, ob die Aktivierungszeit nach der Aktivierung des ersten Geräts endet.

Der Wert, den Sie für den Ablauf des Aktivierungskennworts eingeben, wird in den Fenstern „Geräteaktivierungskennwort festlegen“ und „Benutzer hinzufügen“ als Standardeinstellung im Feld „Ablauf des Aktivierungskennworts“ angezeigt.

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Erweitern Sie im linken Fensterbereich die Option **Allgemeine Einstellungen**.
3. Klicken Sie auf **Standards der Aktivierung**.
4. Geben Sie im Feld **Ablauf des Aktivierungskennworts** die Standardzeit ein, die ein Aktivierungskennwort gültig bleibt, bevor es abläuft. Die Standardzeit kann 1 Minute bis 30 Tage betragen.
5. Bei Bedarf aktivieren Sie das Kontrollkästchen **Aktivierungszeitraum endet nach der Aktivierung des ersten Geräts**.

6. Ändern Sie im Feld **Länge des automatisch generierten Aktivierungskennworts** den Wert, sodass er der Länge des automatisch generierten Aktivierungskennworts entspricht. Ein Wert von 4 bis 16 ist zulässig.
7. Aktivieren oder deaktivieren Sie die Option **Registrierung mit BlackBerry Infrastructure einschalten**, um zu ändern, wie Benutzer ihre Mobilgeräte aktivieren. Wenn Sie diese Option deaktivieren, werden die Benutzer bei der Geräteaktivierung aufgefordert, die Serveradresse für BES12 anzugeben. Weitere Informationen finden Sie unter „Abschalten der Benutzerregistrierung bei der BlackBerry Infrastructure“.
8. Klicken Sie auf **Speichern**.

Abschalten der Benutzerregistrierung bei der BlackBerry Infrastructure

Die Registrierung bei der BlackBerry Infrastructure vereinfacht die Aktivierung von Mobilgeräten. Wenn die Registrierung eingeschaltet ist, müssen die Benutzer keine Serveradresse beim Aktivieren des Gerätes eingeben. Wenn Sie diese Einstellung ändern, müssen Sie die Aktivierungs-E-Mail ggf. mit dem gleichen Vorgang aktualisieren, mit dem Benutzer ihre Geräte aktivieren.

Die Registrierung ist standardmäßig aktiviert. Sie müssen jedoch die Kommunikation mit der BlackBerry Infrastructure per SSL aktivieren, damit die Registrierung erfolgreich durchgeführt werden kann.

Geräte mit BlackBerry OS (Version 5.0 bis 7.1) kontaktieren die BlackBerry Infrastructure nicht. Daher ändert sich der Aktivierungsvorgang für diese Geräte durch das Ein- oder Ausschalten der Benutzerregistrierung nicht.

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Erweitern Sie im linken Fensterbereich die Option **Allgemeine Einstellungen**.
3. Klicken Sie auf **Standards der Aktivierung**.
4. Deaktivieren Sie das Kontrollkästchen **Registrierung mit BlackBerry Infrastructure einschalten**.
5. Klicken Sie auf **Speichern**.

Unterstützen von Android for Work-Aktivierungen

Je nach Art Ihrer Google-Domäne und abhängig davon, ob Sie die Erstellung von Benutzerkonten in der Google-Domäne durch BES12 zulassen, müssen Sie zur Unterstützung von Geräteaktivierungen unterschiedliche Schritte durchführen.

- Wenn Sie eine Google Apps for Work-Domäne haben, konsultieren Sie den Abschnitt „Unterstützen von Android for Work-Aktivierungen mit einer Google Apps for Work-Domäne“.
- Wenn Sie eine Google for Work-Domäne haben, konsultieren Sie den Abschnitt „Unterstützen von Android for Work-Aktivierungen mit einer Google for Work-Domäne“.

Verwandte Informationen

Unterstützen von Android for Work-Aktivierungen mit einer Google Apps for Work-Domäne, auf Seite 244
Unterstützen von Android for Work-Aktivierungen mit einer Google for Work-Domäne, auf Seite 244

Unterstützen von Android for Work-Aktivierungen mit einer Google Apps for Work-Domäne

Wenn Sie BES12 für eine Verbindung mit einer Google Apps for Work-Domäne konfiguriert haben, müssen Sie die folgenden Aufgaben ausführen, damit Benutzer Geräte mit einer Android for Work-Aktivierungsart aktivieren können.

Bevor Sie beginnen:

- Stellen Sie sicher, dass eine Google Apps for Work-Domäne vorhanden ist. Informationen zum Erstellen einer Google Apps for Work-Domäne finden Sie unter https://www.google.com/a/signup.
- Konfigurieren Sie BES12 zur Unterstützung von Android for Work. Weitere Informationen über das Konfigurieren von BES12 zur Unterstützung von Android for Work finden Sie in der Dokumentation zur Konfiguration unter help.blackberry.com/detectLang/bes12/.

1. Erstellen Sie in der Google Apps for Work-Domäne Benutzerkonten für die Android for Work-Benutzer.
2. Erstellen Sie in BES12 lokale Benutzerkonten für die Android for Work-Benutzer. Die E-Mail-Adressen der einzelnen Konten müssen mit denen der zugehörigen Google Apps for Work-Konten übereinstimmen.
3. Stellen Sie sicher, dass die Benutzer das Kennwort für ihr Google Apps for Work-Konto kennen.
4. Stellen Sie sicher, dass die Android for Work-Benutzer auf Unternehmensressourcen zugreifen können, indem Sie ihnen ein E-Mail-Profil und die App-Gruppe „Empfohlene Android for Work-Apps“ zuweisen.

Unterstützen von Android for Work-Aktivierungen mit einer Google for Work-Domäne

Wenn Sie BES12 für die Verbindung mit einer Google for Work-Domäne konfigurieren, müssen Sie entscheiden, ob die Erstellung von Benutzerkonten durch BES12 in dieser Google for Work-Domäne zugelassen werden soll. Von dieser Entscheidung hängt ab, welche Aufgaben Sie ausführen müssen, damit Benutzer Geräte mit einer Android for WorkAktivierungsart aktivieren können.

Bevor Sie beginnen:

- Stellen Sie sicher, dass eine Google for Work-Domäne vorhanden ist. Informationen zum Erstellen einer Google for Work-Domäne finden Sie unter https://www.google.com/a/signup.
- Konfigurieren Sie BES12 zur Unterstützung von Android for Work. Weitere Informationen über das Konfigurieren von BES12 zur Unterstützung von Android for Work finden Sie in der Dokumentation zur Konfiguration unter http://help.blackberry.com/detectLang/bes12/.

Aufgaben, wenn BES12 keine Benutzerkonten in der Google for Work-Domäne erstellen kann

Wenn Sie nicht zulassen, dass BES12 in Ihrer Google for Work-Domäne Benutzerkonten erstellt, müssen Sie in der Google for Work-Domäne und in BES12 Benutzerkonten erstellen.

1. Fügen Sie in BES12 Verzeichnis-Benutzerkonten für die Android for Work-Benutzer hinzu.
2. Erstellen Sie in der Google for Work-Domäne Benutzerkonten für die Android for Work-Benutzer. Die E-Mail-Adressen der jeweiligen Konten müssen mit denen der zugehörigen BES12-Benutzerkonten übereinstimmen.
    a. Synchronisieren Sie optional mit Google Apps Directory Sync Ihre Google for Work-Domäne mit Ihrem Unternehmensverzeichnis. Wenn Sie dies tun, müssen Sie keine Benutzerkonten in Ihrer Google for Work-Domäne manuell erstellen.
3. Stellen Sie sicher, dass die Android for Work-Benutzer das Kennwort für ihr Google for Work-Konto kennen.
4. Damit die Android for Work-Benutzer auf Unternehmensressourcen zugreifen können, weisen Sie ihnen ein E-Mail-Profil und die App-Gruppe „Empfohlene Android for Work-Apps“ zu.

Aufgaben, wenn BES12 Benutzerkonten in der Google for Work-Domäne erstellen kann

Wenn Sie die Erstellung von Benutzerkonten durch BES12 in Ihrer Google for Work-Domäne zulassen, erstellt BES12 ein Google for Work-Konto, wenn ein neuer Benutzer ein Gerät aktiviert. BES12 sendet das Kennwort für das neue Konto an die E-Mail-Adresse des Benutzers. Wenn Sie diese Option wählen, stellen Sie sicher, dass Sie das Google-Dienstkonto in der Google for Work-Domäne so konfiguriert haben, dass BES12 Benutzerkonten erstellen kann. Weitere Informationen zum Zulassen der Erstellung von Benutzerkonten durch das Google-Dienstkonto finden Sie in der Dokumentation zur Konfiguration unter http://help.blackberry.com/detectLang/bes12/.

1. Fügen Sie in BES12 Verzeichnis-Benutzerkonten für die Android for Work-Benutzer hinzu.
2. Damit die Android for Work-Benutzer auf Unternehmensressourcen zugreifen können, weisen Sie ihnen ein E-Mail-Profil und die App-Gruppe „Empfohlene Android for Work-Apps“ zu.

Verwalten von Vorlagen für die Aktivierungs-E-Mail

Sie können mehrere Vorlagen für Aktivierungs-E-Mail erstellen, diese für bestimmte Gerätetypen oder Benutzergruppen anpassen und jedem Benutzerkonto die geeignete Vorlage zuweisen. Wenn Sie ein Aktivierungskennwort für ein Konto festlegen, versendet BES12 eine personalisierte Aktivierungs-E-Mail auf der Grundlage der zugewiesenen Vorlage. Sie können jede Vorlage mit Variablen anpassen, unterschiedliche Vorlagen mit detaillierten Anweisungen zum Aktivieren des jeweiligen Gerätetyps erstellen und zwei E-Mails verwenden, um das Aktivierungskennwort und den Rest der Aktivierungsinformationen getrennt zu versenden.

BES12 enthält eine Standardvorlage für Aktivierungs-E-Mail, die nicht gelöscht werden kann. Sie können die Standardvorlage nach Bedarf bearbeiten. Wenn Sie einem Benutzerkonto keine andere Vorlage zuweisen, verwendet BES12 die Standardvorlage beim Versand der Aktivierungs-E-Mail an das Benutzerkonto.

Erstellen einer Vorlage für Aktivierungs-E-Mail

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Erweitern Sie im linken Fensterbereich die Option **Allgemeine Einstellungen**.
3. Klicken Sie auf **Aktivierungs-E-Mail**.
4. Klicken Sie auf +.
5. Geben Sie im Feld **Name** einen Namen für die Vorlage ein.
6. Bearbeiten Sie den Text im Feld **Betreff** zum Anpassen der Betreffzeile der ersten Aktivierungs-E-Mail.
7. Ändern Sie den Text der Aktivierungs-E-Mail-Nachricht, die Sie an Benutzer senden. Klicken Sie auf **Textvorschlag**, um einen Beispielnachrichtentext anzuzeigen, den Sie für verschiedene Benutzer anpassen können. Wenn Sie entscheiden, nur eine Aktivierungs-E-Mail-Nachricht zu senden, nehmen Sie unbedingt das Aktivierungskennwort in diese auf. Sie können Variablen im Text verwenden, um die E-Mail-Nachricht für verschiedene Benutzer anzupassen. Eine Liste von Variablen finden Sie unter „Standardvariablen“.
8. Wählen Sie **Zwei Aktivierungs-E-Mails senden – die Erste mit allen Anweisungen, die Zweite mit dem Kennwort** aus, um eine zweite Aktivierungs-E-Mail-Nachricht zu erstellen, damit Sie das Aktivierungskennwort getrennt von den Aktivierungsanweisungen senden können.
9. Geben Sie im Feld **Betreff** eine Betreffzeile für die zweite Aktivierungs-E-Mail ein.
10. Ändern Sie den Text der zweiten Aktivierungs-E-Mail-Nachricht, die Sie an Benutzer senden. Nehmen Sie darin unbedingt das Aktivierungskennwort auf.
11. Klicken Sie auf **Speichern**.

Bearbeiten einer Vorlage für Aktivierungs-E-Mail

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Erweitern Sie im linken Fensterbereich die Option **Allgemeine Einstellungen**.
3. Klicken Sie auf **Aktivierungs-E-Mail**.
4. Klicken Sie auf **Standardmäßige Aktivierungs-E-Mail**.
5. Geben Sie im ersten Feld **Betreff** eine Betreffzeile für die erste Aktivierungs-E-Mail ein.
6. Ändern Sie den Text der Aktivierungs-E-Mail-Nachricht, die Sie an Benutzer senden. Klicken Sie auf **Textvorschlag**, um einen Beispielnachrichtentext anzuzeigen, den Sie für verschiedene Benutzer anpassen können. Wenn Sie entscheiden, nur eine Aktivierungs-E-Mail-Nachricht zu senden, nehmen Sie unbedingt das Aktivierungskennwort in diese auf. Sie können Variablen im Text verwenden, um die E-Mail-Nachricht für verschiedene Benutzer anzupassen. Eine Liste von Variablen finden Sie unter „Standardvariablen“.
7. Wählen Sie **Zwei Aktivierungs-E-Mails senden – die Erste mit allen Anweisungen, die Zweite mit dem Kennwort** aus, um eine zweite Aktivierungs-E-Mail-Nachricht zu erstellen, damit Sie das Aktivierungskennwort getrennt von den Aktivierungsanweisungen senden können.

8. Geben Sie im Feld **Betreff** eine Betreffzeile für die zweite Aktivierungs-E-Mail ein.
9. Ändern Sie den Text der zweiten Aktivierungs-E-Mail-Nachricht, die Sie an Benutzer senden. Nehmen Sie darin unbedingt das Aktivierungskennwort auf.
10. Klicken Sie auf **Speichern**.

Steuern der Geräteaktivierungseinstellungen mithilfe von Aktivierungsprofilen

Mithilfe von Aktivierungsprofilen können Sie steuern, wie die Geräte aktiviert und verwaltet werden. Ein Aktivierungsprofil gibt an, wie viele Geräte und welche Gerätetypen ein Benutzer aktivieren kann, ob auf Geräten ein separater geschäftlicher Bereich installiert ist und wie Sie geschäftliche und persönliche Daten auf dem Gerät verwalten dürfen.

Das zugewiesene Profil gilt nur für Geräte, die der Benutzer aktiviert, nachdem Sie ihm das Profil zugewiesen haben. Geräte, die bereits aktiviert sind, werden nicht automatisch aktualisiert, um dem neuen oder aktualisierten Aktivierungsprofil zu entsprechen.

Wenn Sie in BES12 einen Benutzer hinzufügen, wird dem Benutzerkonto das Standard-Aktivierungsprofil zugewiesen. Sie können das Standard-Aktivierungsprofil entsprechend Ihrer Anforderungen ändern, oder Sie können ein benutzerdefiniertes Aktivierungsprofil erstellen und dieses Benutzern oder Benutzergruppen zuweisen.

Die Aktivierungprofile gelten nicht für Geräte mit BlackBerry OS (Version 5.0 bis 7.1).

Verwenden von Aktivierungsarten für die Konfiguration der Kontrolle über Geräte

Sie können Aktivierungsarten verwenden, um zu konfigurieren, wie viel Kontrolle Sie über aktivierte Geräte haben. Diese Flexibilität bei der Kontrolle ist hilfreich, wenn Sie volle Kontrolle über ein Gerät haben möchten, das Sie einem Benutzer ausgeben, oder wenn Sie sicherstellen möchten, dass Sie keine Kontrolle über die privaten Daten eines Geräts haben, das dem Benutzer gehört und das er mit in die Arbeit bringt. In den nachfolgenden Tabellen sind die für Geräte verfügbaren Aktivierungsarten aufgeführt.

Die Aktivierungsarten gelten nicht für Geräte mit BlackBerry OS (Version 5.0 bis 7.1). Sie können die IT-Richtlinien von BlackBerry OS in der IT-Richtliniengruppe „Persönliche Geräte“ verwenden, um zwischen geschäftlichen und persönlichen Inhalten auf dem Gerät zu unterscheiden. Weitere Informationen finden Sie in der Richtlinien-Referenztabelle unter help.blackberry.com/detectLang/bes12/current/policy-reference-spreadsheet-zip/.

BlackBerry 10-Geräte

Aktivierungsart	Beschreibung
Geschäftlich und persönlich – Unternehmen	Die Aktivierungsart ermöglicht die Steuerung von geschäftlichen Daten auf dem Gerät und stellt gleichzeitig sicher, dass private Daten geschützt werden. Wenn ein Gerät aktiviert wird, wird auf dem Gerät ein separater geschäftlicher Bereich

Aktivierungsart	Beschreibung
	erstellt, und der Benutzer muss ein Kennwort erstellen, um auf den geschäftlichen Bereich zuzugreifen. Geschäftsdaten werden über Verschlüsselung und Kennwortauthentifizierung geschützt. Alle geschäftlichen Daten von vorherigen Aktivierungen werden gelöscht. Mithilfe von IT-Administrationsbefehlen und IT-Richtlinien können Sie den geschäftlichen Bereich des Geräts steuern, jedoch nicht den privaten Bereich des Geräts.
Nur geschäftlicher Bereich	Diese Aktivierungsart ermöglicht eine vollständige Kontrolle über das Gerät und bietet keinen separaten Bereich für persönliche Daten. Wenn ein Gerät aktiviert wird, werden der persönliche Bereich sowie alle geschäftlichen Daten von vorherigen Aktivierungen entfernt, und es wird ein geschäftlicher Bereich erstellt. Der Benutzer muss ein Kennwort einrichten, um auf das Gerät zuzugreifen. Geschäftsdaten werden über Verschlüsselung und Kennwortauthentifizierung geschützt. Sie können das Gerät mithilfe von IT-Administrationsbefehlen und IT-Richtlinien steuern.
Geschäftlich und persönlich – Reguliert	Diese Aktivierungsart ermöglicht die Kontrolle über die geschäftlichen und die persönlichen Daten. Wenn ein Gerät aktiviert wird, wird auf dem Gerät ein separater geschäftlicher Bereich erstellt, und der Benutzer muss ein Kennwort erstellen, um auf den geschäftlichen Bereich zuzugreifen. Geschäftsdaten werden über Verschlüsselung und Kennwortauthentifizierung geschützt. Alle geschäftlichen Daten von vorherigen Aktivierungen werden gelöscht. Sie können sowohl den geschäftlichen als auch den persönlichen Bereich auf dem Gerät mit IT-Administrationsbefehlen und IT-Richtlinien steuern.

iOS-Geräte

Aktivierungsart	Beschreibung
MDM-Steuerelemente	Diese Aktivierungsart stellt eine grundlegende Geräteverwaltung mithilfe der durch iOS und Windows Phone zur Verfügung gestellten Gerätesteuerelemente bereit. Es wird kein separater geschäftlicher Bereich auf dem Gerät installiert, und es gibt keine zusätzliche Sicherheit für geschäftliche Daten. Sie können das Gerät mithilfe von IT-Administrationsbefehlen und IT-Richtlinien steuern. Während der Aktivierung müssen Benutzer ein Mobilgeräteverwaltungsprofil auf ihrem Gerät installieren.
Geschäftlich und persönlich – vollständige Kontrolle	Diese Aktivierungsart stellt die volle Kontrolle über Geräte bereit. Wenn ein Gerät aktiviert wird, wird auf dem Gerät ein separater geschäftlicher Bereich

Aktivierungsart	Beschreibung
	erstellt, und der Benutzer muss ein Kennwort erstellen, um auf den geschäftlichen Bereich zuzugreifen. Geschäftsdaten werden über Verschlüsselung und Kennwortauthentifizierung geschützt. Mithilfe von IT-Administrationsbefehlen und IT-Richtlinien können Sie den geschäftlichen Bereich und einige weitere Aspekte des Geräts steuern, die sowohl den privaten als auch den geschäftlichen Bereich des Geräts betreffen. Während der Aktivierung müssen Benutzer ein Mobilgeräteverwaltungsprofil installieren.
Geschäftlich und persönlich – Benutzer-Datenschutz	Die Aktivierungsart ermöglicht die Steuerung von geschäftlichen Daten auf dem Gerät und stellt gleichzeitig sicher, dass private Daten geschützt werden. Wenn ein Gerät aktiviert wird, wird auf dem Gerät ein separater geschäftlicher Bereich erstellt, und der Benutzer muss ein Kennwort erstellen, um auf den geschäftlichen Bereich zuzugreifen. Geschäftsdaten werden über Verschlüsselung und Kennwortauthentifizierung geschützt. Mithilfe von IT-Administrationsbefehlen und IT-Richtlinien können Sie den geschäftlichen Bereich des Geräts steuern, jedoch nicht den privaten Bereich des Geräts. Benutzer müssen kein Mobilgeräteverwaltungsprofil installieren.

Windows Phone-Geräte

Aktivierungsart	Beschreibung
MDM-Steuerelemente	Diese Aktivierungsart stellt eine grundlegende Geräteverwaltung über die von Windows Phone zur Verfügung gestellten Gerätesteuerelemente bereit. Es wird kein separater geschäftlicher Bereich auf dem Gerät installiert, und es gibt keine zusätzliche Sicherheit für geschäftliche Daten. Sie können das Gerät mithilfe von IT-Administrationsbefehlen und IT-Richtlinien steuern. Während der Aktivierung müssen Benutzer ihre Geräte über die Windows Phone-Unternehmens-Apps installieren.

Android-Geräte

Wenn Sie die Aktivierungsart für Android-Geräte konfigurieren, können Sie mehrere Aktivierungsarten auswählen und ihnen eine Reihenfolge zuweisen, um sicherzustellen, dass BES12 die am besten geeignete Aktivierungsart für dieses Gerät zuweist. Wenn Sie beispielsweise „Nur geschäftlicher Bereich (Samsung KNOX)“ den ersten Rang und „MDM-Steuerelemente“ den zweiten zuweisen, wird für Geräte, die KNOX Workspace unterstützen, die erste Aktivierungsart verwendet.

Hinweis: KNOX MDM ermöglicht die Verwendung von KNOX MDM IT-Richtlinienregeln in BES12 auf Geräten anstelle der einfachen, für alle Android-Geräte verfügbaren Regeln. KNOX Workspace erstellt auf dem Gerät einen separaten geschäftlichen Bereich, sodass geschäftliche und private Daten und Apps voneinander getrennt bleiben.

Aktivierungsart	Beschreibung
MDM-Steuerelemente	Diese Aktivierungsart gilt für: • Android-Geräte, einschließlich Samsung-Geräten, die KNOX MDM unterstützen Diese Aktivierungsart ermöglicht die Verwaltung von Geräten über IT-Administrationsbefehle und IT-Richtlinienregeln. Wenn ein Gerät KNOX MDM unterstützt, wendet diese Aktivierungsart die KNOX MDM IT-Richtlinienregeln an. Es wird kein separater geschäftlicher Bereich auf dem Gerät installiert, und es gibt keine zusätzliche Sicherheit für geschäftliche Daten. Während der Aktivierung müssen Benutzer dem BES12 Client Administratorberechtigungen erteilen.
Geschäftlich und persönlich – vollständige Kontrolle (Secure Work Space)	Diese Aktivierungsart gilt für: • Android-Geräte, einschließlich Samsung-Geräten, die KNOX MDM unterstützen Diese Aktivierungsart ermöglicht die Verwaltung des gesamten Geräts über IT-Administrationsbefehle und IT-Richtlinienregeln. Wenn ein Gerät KNOX MDM unterstützt, werden die KNOX MDM IT-Richtlinienregeln angewendet. Die Aktivierungsart erstellt einen separaten geschäftlichen Bereich, und der Benutzer muss ein Kennwort einrichten, um auf diesen zuzugreifen. Daten im geschäftlichen Bereich werden über Verschlüsselung und Kennwortauthentifizierung geschützt. Während der Aktivierung müssen Benutzer dem BES12 Client Administratorberechtigungen erteilen.
Geschäftlich und persönlich – Benutzer-Datenschutz (Secure Work Space)	Diese Aktivierungsart gilt für: • Android-Geräte Diese Aktivierungsart bietet Datenschutz für persönliche Daten, ermöglicht Ihnen jedoch die Verwaltung geschäftlicher Daten mit IT-Administrationsbefehlen und IT-Richtlinienregeln. Diese Aktivierungsart unterstützt die KNOX MDM IT-Richtlinienregeln nicht. Die Aktivierungsart erstellt einen separaten geschäftlichen Bereich, und der Benutzer muss ein Kennwort einrichten, um auf diesen zuzugreifen. Daten im geschäftlichen Bereich werden über Verschlüsselung und Kennwortauthentifizierung geschützt. Die Benutzer müssen dem BES12 Client keine Administratorberechtigungen erteilen.

Aktivierungsart	Beschreibung
Geschäftlich und persönlich – vollständige Kontrolle (Samsung KNOX)	Diese Aktivierungsart gilt für: • Samsung-Geräte, die KNOX Workspace unterstützen Diese Aktivierungsart ermöglicht die Verwaltung des gesamten Geräts über IT-Administrationsbefehle und die KNOX MDM- sowie KNOX Workspace IT-Richtlinienregeln. Die Aktivierungsart erstellt einen separaten geschäftlichen Bereich, und der Benutzer muss ein Kennwort einrichten, um auf diesen zuzugreifen. Daten im geschäftlichen Bereich werden durch Verschlüsselung und eine Methode zur Authentifizierung, beispielsweise Kennwort, PIN, Muster oder Fingerabdruck, geschützt. Während der Aktivierung müssen Benutzer dem BES12 Client Administratorberechtigungen erteilen.
Nur geschäftlicher Bereich - (Samsung KNOX)	Diese Aktivierungsart gilt für: • Samsung-Geräte, die KNOX Workspace unterstützen Diese Aktivierungsart ermöglicht die Verwaltung des gesamten Geräts über IT-Administrationsbefehle und die KNOX MDM- sowie KNOX Workspace IT-Richtlinienregeln. Diese Aktivierungsart entfernt den persönlichen Bereich und installiert einen geschäftlichen Bereich. Der Benutzer muss ein Kennwort für den Zugriff auf das Gerät erstellen. Alle Daten auf dem Gerät werden durch Verschlüsselung und eine Methode zur Authentifizierung, beispielsweise Kennwort, PIN, Muster oder Fingerabdruck, geschützt. Während der Aktivierung müssen Benutzer dem BES12 Client Administratorberechtigungen erteilen.
Geschäftlich und persönlich – Benutzer-Datenschutz (Android for Work)	Diese Aktivierungsart gilt für: • Android-Geräte, die Android for Work unterstützen Diese Aktivierungsart bietet Datenschutz für persönliche Daten, ermöglicht Ihnen jedoch die Verwaltung geschäftlicher Daten mit IT-Administrationsbefehlen und IT-Richtlinienregeln. Diese Aktivierungsart unterstützt die KNOX MDM IT-Richtlinienregeln nicht. Diese Aktivierungsart erstellt ein geschäftliches Profil auf dem Gerät, durch das geschäftliche und persönliche Daten voneinander getrennt werden. Sowohl geschäftliche als auch persönliche Daten werden über Verschlüsselung und Kennwortauthentifizierung geschützt. Diese Aktivierungsart unterstützt BlackBerry Secure Connect Plus nicht. Die Benutzer müssen dem BES12 Client keine Administratorberechtigungen erteilen.

Aktivierungsart	Beschreibung
Geschäftlich und persönlich – Benutzer-Datenschutz (Android for Work - Premium)	Diese Aktivierungsart gilt für: • Android-Geräte, die Android for Work unterstützen Diese Aktivierungsart bietet Datenschutz für persönliche Daten, ermöglicht Ihnen jedoch die Verwaltung geschäftlicher Daten mit IT-Administrationsbefehlen und IT-Richtlinienregeln. Diese Aktivierungsart unterstützt die KNOX MDM IT-Richtlinienregeln nicht. Diese Aktivierungsart erstellt ein geschäftliches Profil auf dem Gerät, durch das geschäftliche und persönliche Daten voneinander getrennt werden. Sowohl geschäftliche als auch persönliche Daten werden über Verschlüsselung und Kennwortauthentifizierung geschützt. Diese Aktivierungsart müssen Sie verwenden, wenn Sie BlackBerry Secure Connect Plus unterstützen möchten. Die Benutzer müssen dem BES12 Client keine Administratorberechtigungen erteilen.

Erstellen eines Aktivierungsprofils

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf + neben **Aktivierung**.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
4. Im Feld **Anzahl der Geräte, die ein Benutzer aktivieren kann** geben Sie die maximale Anzahl von Geräten ein, die der Benutzer aktivieren kann.
5. Führen Sie in der Dropdown-Liste **Geräteigentümer** eine der folgenden Aktionen aus:
   - Wählen Sie **Nicht angegeben** aus, wenn einige Benutzer persönliche Geräte und einige Benutzer geschäftliche Geräte aktivieren.
   - Wählen Sie **Geschäftlich** aus, wenn Benutzer in der Regel geschäftliche Geräte aktivieren.
   - Wählen Sie **Persönlich** aus, wenn Benutzer in der Regel persönliche Geräte aktivieren.
6. Wählen Sie die erforderlichen Gerätetypen im Abschnitt **Gerätetypen, die Benutzer aktivieren können** aus oder deaktivieren Sie die jeweilige Option. Deaktivierte Gerätetypen sind nicht im Aktivierungsprofil enthalten und können von Benutzern, die diesem Aktivierungsprofil zugewiesen wurden, nicht aktiviert werden.
7. Führen Sie die folgenden Schritte für jeden Gerätetyp aus, der Teil des Aktivierungsprofils sein soll:
   - Klicken Sie auf die Registerkarte für den Gerätetyp.
   - Wählen Sie in der Dropdown-Liste **Gerätemodell-Einschränkungen** aus, ob nur bestimmte Geräte erlaubt oder beschränkt werden oder ob keinerlei Einschränkungen gelten sollen. Wenn Sie eine andere Option als **Keine**

Einschränkungen gewählt haben, klicken Sie auf **Bearbeiten**, wählen Sie die zu erlaubenden oder einzuschränkenden Geräte aus und klicken Sie auf **Speichern**.

- In der Dropdown-Liste **Zugelassene Version** wählen Sie die zumindest zugelassene Version aus.
- Im Abschnitt **Aktivierungstyp** wählen Sie einen Aktivierungstyp aus.
- Optional können Sie auf der Registerkarte **BlackBerry** einen Organisationshinweis in der Dropdown-Liste **Organisationshinweis zuweisen** auswählen.
- Optional können Sie auf der Registerkarte **Android** den Aktivierungsarten eine Rangfolge zuweisen, damit sie den Anforderungen Ihrer Organisation entsprechen.

8. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Weisen Sie Profilen einen Rang zu.

Einrichten eines Aktivierungskennworts und Senden einer Aktivierungs-E-Mail-Nachricht

Sie können ein Aktivierungskennwort einrichten und einem Benutzer eine Aktivierungs-E-Mail mit den erforderlichen Informationen senden, um ein BlackBerry OS-Gerät (Version 5.0 bis 7.1) und eines oder mehrere BlackBerry 10-, iOS-, Android- oder Windows Phone-Geräte zu aktivieren.

Bevor Sie beginnen: Aktualisieren Sie die Vorlage für die Aktivierungs-E-Mail-Nachricht.

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte**.
2. Suchen Sie nach einem Benutzerkonto.
3. Klicken Sie in den Suchergebnissen auf den Namen des Benutzerkontos.
4. Klicken Sie im Bereich „Benutzerdaten“ auf **Aktivierungskennwort festlegen**.
5. Führen Sie im Fenster **Geräteaktivierungskennwort festlegen** eine der folgenden Aktionen aus:

Aufgabe	Schritt
Generieren Sie automatisch ein Aktivierungskennwort für das Benutzerkonto, und senden Sie die Aktivierungs-E-Mail.	1. Klicken Sie auf **Automatisch ein Geräteaktivierungskennwort generieren und eine E-Mail mit Aktivierungsanweisungen senden**. 2. Wählen Sie im Feld **Ablauf des Aktivierungszeitraums** die Zeitdauer aus, für die ein Aktivierungskennwort gültig bleibt. 3. Klicken Sie in der Dropdown-Liste **Vorlage für Aktivierungs-E-Mail** auf eine Vorlage für die Aktivierungs-E-Mail für den Benutzer.
Richten Sie das Aktivierungskennwort für das	1. Klicken Sie auf **Aktivierungskennwort festlegen**.

Aufgabe	Schritt
Benutzerkonto ein, und senden Sie bei Bedarf die Aktivierungs-E-Mail.	2. Geben Sie das Aktivierungskennwort ein. Klicken Sie auf , um den Text im Feld **Aktivierungskennwort für das Gerät** anzuzeigen. 3. Wählen Sie im Feld **Ablauf des Aktivierungszeitraums** die Zeitdauer aus, für die ein Aktivierungskennwort gültig bleibt. 4. Aktivieren Sie bei Bedarf das Kontrollkästchen **E-Mail mit Aktivierungsanweisungen und Aktivierungskennwort senden**. Falls Sie diese Option nicht auswählen, müssen Sie dem Benutzer das Kennwort selbst mitteilen. 5. Klicken Sie in der Dropdown-Liste **Vorlage für Aktivierungs-E-Mail** auf eine Vorlage für die Aktivierungs-E-Mail für den Benutzer.

6. Klicken Sie auf **Speichern**.

Zulassen, dass Benutzer Aktivierungskennwörter festlegen

Benutzer können Aktivierungskennwörter erstellen, um Geräte über das kabellose Netzwerk zu aktivieren.

Gerät	Zu verwendender Dienst
BlackBerry 10	BES12 Self-Service
iOS	BES12 Self-Service
Android	BES12 Self-Service
Windows Phone	BES12 Self-Service
BlackBerry OS (Version 5.0 bis 7.1)	BlackBerry Web Desktop Manager

Weitere Informationen finden Sie im das BES12 Self-Service-Benutzerhandbuch unter help.blackberry.com/detectlang/bes12-self-service/latest/bes12-self-service-pdf.

Weitere Informationen zu BlackBerry Web Desktop Manager finden Sie im Benutzerhandbuch zu BlackBerry Web Desktop Manager.

Aktivieren eines BlackBerry 10-Geräts

Senden Sie die folgenden Aktivierungsanweisungen an den Gerätebenutzer.

1. Navigieren Sie auf dem Gerät zu **Einstellungen**.
2. Tippen Sie auf **Konten**.

3. Wenn Sie auf diesem Gerät über vorhandene Konten verfügen, tippen Sie auf **Konto hinzufügen**. Andernfalls fahren Sie mit Schritt 4 fort.
4. Tippen Sie auf **E-Mail, Kalender und Kontakte**.
5. Geben Sie Ihre geschäftliche E-Mail-Adresse ein, und tippen Sie auf **Weiter**.
6. Geben Sie im Feld **Kennwort** das empfangene Aktivierungskennwort ein. Tippen Sie auf **Weiter**.
7. Wenn Sie anhand einer Warnmeldung informiert werden, dass Ihr Gerät die Verbindungsinformationen nicht finden konnte, führen Sie die folgenden Schritte aus:
   a. Tippen Sie auf **OK**.
   b. Tippen Sie auf **Erweitert**.
   c. Tippen Sie auf **Geschäftliches Konto**.
   d. Geben Sie im Feld **Serveradresse** die Adresse des Servers ein. Tippen Sie auf **Fertig**. Die Serveradresse finden Sie entweder in der Aktivierungs-E-Mail-Nachricht, die Ihnen zugesendet wurde, oder in BES12 Self-Service.
8. Folgen Sie den Anweisungen auf dem Bildschirm, um den Aktivierungsprozess abzuschließen.

Wenn Sie fertig sind: Um zu überprüfen, ob der Aktivierungsprozess erfolgreich abgeschlossen wurde, führen Sie eine der folgenden Aktionen aus:

- Navigieren Sie auf dem Gerät zum BlackBerry Hub, und bestätigen Sie, dass die E-Mail-Adresse vorhanden ist. Navigieren Sie zum Kalender, und bestätigen Sie, dass die Kalendertermine vorhanden sind.
- Überprüfen Sie in BES12 Self-Service, ob Ihr Gerät als aktiviertes Gerät aufgeführt ist. Nachdem Sie das Gerät aktiviert haben, kann es bis zu zwei Minuten dauern, bis der Status aktualisiert wird.

Aktivieren eines BlackBerry OS-Geräts

Senden Sie die folgenden Aktivierungsanweisungen an den Gerätebenutzer.

1. Navigieren Sie auf dem Gerät zu **Setup**.
2. Klicken Sie auf **E-Mail-Konten**.
3. Klicken Sie auf **Enterprise-Konto**.
4. Geben Sie im Feld **E-Mail** Ihre geschäftliche E-Mail-Adresse ein.
5. Geben Sie im Feld **Kennwort** das empfangene Aktivierungskennwort ein.
6. Klicken Sie auf **Aktivieren**.
7. Klicken Sie auf **OK**.

Wenn Sie fertig sind: Um zu überprüfen, ob der Aktivierungsprozess erfolgreich abgeschlossen wurde, führen Sie eine der folgenden Aktionen aus:

- Navigieren Sie auf dem Gerät zur Setup-App, und klicken Sie auf **E-Mail-Konten**. Bestätigen Sie, dass die E-Mail-Adresse vorhanden ist.

- Überprüfen Sie in BlackBerry Web Desktop Manager, ob Ihr Gerät als aktiviertes Gerät aufgeführt ist. Nachdem Sie das Gerät aktiviert haben, kann es bis zu zwei Minuten dauern, bis der Status aktualisiert wird.

Aktivieren eines iOS-Geräts

Senden Sie die folgenden Aktivierungsanweisungen an den Gerätebenutzer.

Hinweis: Diese Schritte gelten für Geräte, denen die MDM-Steuerelemente-Aktivierungsart zugewiesen ist. Bei Aktivierungsarten, mit denen ein geschäftlicher Bereich auf Geräten installiert oder aktiviert wird, können zusätzliche Schritte erforderlich sein.

1. Installieren Sie BES12 Client auf dem Gerät. Sie können BES12 Client aus dem App Store herunterladen.
2. Tippen Sie auf dem Gerät auf **BES12**.
3. Lesen Sie die Lizenzvereinbarung, und tippen Sie auf **Ich stimme zu**.
4. Geben Sie Ihre geschäftliche E-Mail-Adresse ein, und tippen Sie auf **Start**.
5. Geben Sie ggf. die Serveradresse ein, und tippen Sie auf **Start**. Sie finden die Serveradresse in der Aktivierungs-E-Mail-Nachricht, die Sie erhalten haben, oder in BES12 Self-Service.
6. Bestätigen Sie, dass die auf dem Gerät angezeigten Zertifikatsdaten korrekt sind, und tippen Sie auf **Annehmen**. Falls Ihr Administrator Ihnen die Zertifikatsdaten separat gesendet hat, können Sie die angezeigten Informationen mit den Informationen vergleichen, die Sie erhalten haben.
7. Geben Sie Ihr Aktivierungskennwort ein, und tippen Sie auf **Mein Gerät aktivieren**.
8. Tippen Sie auf **OK**, um das erforderliche Zertifikat zu installieren.
9. Folgen Sie den Anweisungen auf dem Bildschirm, um die Aktivierung abzuschließen.
10. Wenn Sie aufgefordert werden, das Kennwort für Ihr E-Mail-Konto oder das Kennwort für Ihr Gerät einzugeben, folgen Sie den Anweisungen auf dem Bildschirm.

Wenn Sie fertig sind: Um zu überprüfen, dass der Aktivierungsprozess erfolgreich abgeschlossen wurde, führen Sie eine der folgenden Aktionen aus:

- Öffnen Sie den BES12 Client auf dem Gerät, und tippen Sie auf **Info**. Überprüfen Sie in den Abschnitten für das aktivierte Gerät und den Kompatibilitätsstatus, dass die Geräteinformationen und der Aktivierungszeitstempel vorhanden sind.
- In BES12 Self-Service überprüfen Sie, ob Ihr Gerät als aktiviertes Gerät aufgeführt ist. Nach der Aktivierung des Geräts kann es bis zu zwei Minuten dauern, bis der Status aktualisiert wird.

Aktivieren eines Android-Geräts

Senden Sie die folgenden Aktivierungsanweisungen an den Gerätebenutzer.

Hinweis: Diese Schritte gelten für Geräte, denen die MDM-Steuerelemente-Aktivierungsart zugewiesen ist. Bei Aktivierungsarten, mit denen ein geschäftlicher Bereich auf Geräten installiert oder aktiviert wird, können zusätzliche Schritte erforderlich sein.

1. Installieren Sie BES12 Client auf dem Gerät. Sie können BES12 Client aus dem Google Play herunterladen.
2. Tippen Sie auf dem Gerät auf **BES12**.
3. Lesen Sie die Lizenzvereinbarung, und tippen Sie auf **Ich stimme zu**.
4. Geben Sie Ihre geschäftliche E-Mail-Adresse ein, und tippen Sie auf **Weiter**.
5. Geben Sie ggf. die Serveradresse ein, und tippen Sie auf **Weiter**. Sie finden die Serveradresse in der Aktivierungs-E-Mail-Nachricht, die Sie erhalten haben, oder in BES12 Self-Service.
6. Bestätigen Sie, dass die auf dem Gerät angezeigten Zertifikatsdaten korrekt sind, und tippen Sie auf **Annehmen**. Falls Ihr Administrator Ihnen die Zertifikatsdaten separat gesendet hat, können Sie die angezeigten Informationen mit den Informationen vergleichen, die Sie erhalten haben.
7. Geben Sie Ihr Aktivierungskennwort ein, und tippen Sie auf **Mein Gerät aktivieren**.
8. Tippen Sie auf **Weiter**.
9. Tippen Sie auf **Aktivieren**.

Wenn Sie fertig sind: Um zu überprüfen, dass der Aktivierungsprozess erfolgreich abgeschlossen wurde, führen Sie eine der folgenden Aktionen aus:

- Öffnen Sie den BES12 Client auf dem Gerät, und tippen Sie auf **Info**. Überprüfen Sie im Abschnitt für das aktivierte Gerät, dass die Geräteinformationen und der Aktivierungszeitstempel vorhanden sind.
- In BES12 Self-Service überprüfen Sie, ob Ihr Gerät als aktiviertes Gerät aufgeführt ist. Nach der Aktivierung des Geräts kann es bis zu zwei Minuten dauern, bis der Status aktualisiert wird.

Aktivieren eines Windows Phone-Geräts

Senden Sie die folgenden Aktivierungsanweisungen an den Gerätebenutzer.

1. Installieren Sie BES12 Client auf dem Gerät. Sie können BES12 Client aus dem Windows Phone Store herunterladen.
2. Öffnen Sie auf dem Gerät die App-Liste, und tippen Sie auf **BES12**.
3. Lesen Sie die Lizenzvereinbarung, und tippen Sie auf **Ich stimme zu**.
4. Geben Sie Ihre geschäftliche E-Mail-Adresse ein, und tippen Sie auf **Weiter**.
5. Geben Sie ggf. die Serveradresse ein, und tippen Sie auf **Weiter**. Sie finden die Serveradresse in der Aktivierungs-E-Mail-Nachricht, die Sie erhalten haben, oder in BES12 Self-Service.
6. Geben Sie das Aktivierungskennwort, das Sie in der Aktivierungs-E-Mail-Nachricht erhalten haben oder das Sie in BES12 Self-Service festgelegt haben, und tippen Sie auf **Mein Gerät aktivieren**.
7. Tippen Sie auf **kopieren und fortfahren** um die angegebene Serveradresse zu kopieren, und mit der Windows Phone Workplace App fortzufahren.

8. Tippen Sie auf **Konto hinzufügen**.
9. Geben Sie Ihre E-Mail-Adresse ein, und tippen Sie auf **Anmelden**.
10. Tippen Sie mit dem Cursor im Feld „Server“ auf das Symbol **Einfügen**.
11. Tippen Sie auf **Anmelden**.
12. Sollten Sie eine Warnung wegen eines Zertifikats erhalten, tippen Sie auf **Fortfahren**.
13. Lassen Sie die Felder Benutzername und Domäne leer. Geben Sie in das Feld „Passwort“ das Aktivierungspasswort ein, das Sie in der Aktivierungs-E-Mail erhalten haben, oder das Sie in BES12 Self-Service vorgegeben haben. Tippen Sie auf **Anmelden**.
14. Tippen Sie auf **Fertig**.
15. Drücken Sie auf die Taste **Zurück** an Ihrem Windows Phone um zu BES12 Client zurückzukehren.
16. Die Aktivierung wird automatisch ausgeführt.

Wenn Sie fertig sind: Um zu überprüfen, dass der Aktivierungsprozess erfolgreich abgeschlossen wurde, führen Sie eine der folgenden Aktionen aus:

- Öffnen Sie auf dem Gerät die Option BES12 Client, tippen am unteren Bildschirmrand auf das Symbol **Menü** (drei horizontale Punkte), und tippen anschließend auf **Info**. Überprüfen Sie im Abschnitt für das aktivierte Gerät, dass die Geräteinformationen und der Aktivierungszeitstempel vorhanden sind.
- In BES12 Self-Service überprüfen Sie, ob Ihr Gerät als aktiviertes Gerät aufgeführt ist. Nach der Aktivierung des Geräts kann es bis zu zwei Minuten dauern, bis der Status aktualisiert wird.

Aktivieren von BlackBerry 10-Geräten mithilfe von BlackBerry Wired Activation Tool

Das BlackBerry Wired Activation Tool ermöglicht die gleichzeitige Aktivierung mehrerer BlackBerry 10-Geräte unter Verwendung von USB-Verbindungen anstelle von drahtlosen Verbindungen. Die Verwendung dieser Methode kann aus verschiedenen Gründen gewünscht sein:

- Schnelle und einfache Aktivierung mehrerer Geräte gleichzeitig
- Beschränkung der Durchführung von Aktivierungen auf die Obhut von Administratoren
- Aktivieren von Geräten und Konfigurieren von Sicherheitsfunktionen (beispielsweise Anforderungen für die Inhaltsverschlüsselung und VPN-Profile), bevor die Geräte an Benutzer ausgehändigt bzw. mit dem Netzwerk des Unternehmens verbunden werden

Sie können keine Profile und Richtlinien mit dem BlackBerry Wired Activation Tool zuweisen. Profile und Richtlinien müssen Benutzern in der BES12-Verwaltungskonsole vor dem Zuweisen und Aktivieren von Geräten mit dem BlackBerry Wired Activation Tool zugewiesen werden. Allerdings müssen Sie keine Aktivierungskennwörter zum Zuweisen und Aktivieren von Geräten mit dem BlackBerry Wired Activation Tool festlegen.

Zum Aktivieren von Geräten mit dem BlackBerry Wired Activation Tool muss auf diesen BlackBerry 10 OS Version 10.3 oder höher ausgeführt werden.

Installieren des BlackBerry Wired Activation Tool

Bevor Sie beginnen:

- Microsoft Windows 7 oder höher auf dem Computer installiert

Führen Sie die folgenden Schritte zum Herunterladen und Installieren des BlackBerry Wired Activation Tool durch:

1. Navigieren Sie zu docs.blackberry.com/bes12tools.
2. Klicken Sie in der Dropdown-Liste auf BlackBerry Wired Activation Tool.
3. Klicken Sie auf **Weiter**.
4. Klicken Sie auf **Download**.
5. Wählen Sie „Ja“ oder „Nein“, und klicken Sie auf **Download**.
6. Speichern Sie die Installationsdatei auf Ihrem Computer.
7. Wechseln Sie auf Ihrem Computer zu dem Ordner, in dem Sie die Installationsdatei gespeichert haben.
8. Folgen Sie den Anweisungen auf dem Bildschirm, um die Installation durchzuführen.

Konfigurieren Sie das BlackBerry Wired Activation Tool, und melden Sie sich bei einer BES12-Instanz an.

Bevor Sie Geräte mit dem BlackBerry Wired Activation Tool aktivieren können, müssen Sie für jede BES12-Instanz, auf die Sie zugreifen müssen, eine Konfiguration erstellen. Nachdem Sie eine Konfiguration erstellt haben, müssen Sie zudem ein Administratorkonto verwenden, damit das BlackBerry Wired Activation Tool auf BlackBerry Web Services zugreifen kann.

1. Doppelklicken Sie im BlackBerry Wired Activation Tool-Installationsordner auf die Datei **BWAT.exe**.
2. Geben Sie im Bildschirm **BES12-Server hinzufügen** im Feld **Name** einen Namen für die Konfiguration ein, die Sie erstellen. Wenn Sie z. B. zwei BES12-Instanzen haben, erstellen Sie für jede eine Konfiguration, und nennen Sie diese „Server 1“ und „Server 2“.
3. Geben Sie im Feld **BlackBerry Web Services-URL** die Webadresse der BlackBerry Web Services-Komponente ein. Standardmäßig ist die Adresse für BlackBerry Web Services „https://<*BES12 web address*>:18084“.

   Sie können den Port durch Ändern der Einstellung tomcat.bws.port in der BES12-Datenbank wechseln.
4. Geben Sie im Feld **BCP-Endpunkt-URL** die Adresse für Geräteaktivierungen ein. Diese wird auch als „Aktivierungs-URL“ bzw. „Servername“ bezeichnet. Wenn Sie die Adresse ermitteln möchten, vergewissern Sie sich, dass die Variable %ActivationURL% in der Vorlage für die Aktivierungs-E-Mail vorhanden ist, und klicken Sie in einem beliebigen Benutzer-Zusammenfassungsbildschirm auf **Aktivierungs-E-Mail anzeigen**.

Falls erforderlich, können Sie auch die Hostadresse und den Port in der BES12-Datenbank nachsehen. Suchen Sie in der Tabelle def_cfg_setting_dfn die Werte id_setting_definition für bdmi.enroll.bcp.host und bdmi.enroll.bcp.port. Verwenden Sie dann die id_setting_definition-Werte zum Ermitteln der Werte dieser Einstellungen in obj_global_cfg_setting.

5. Klicken Sie auf **Senden**.
6. Wählen Sie im Bildschirm **Anmelden** eine BES12-Konfiguration aus der Dropdown-Liste aus.
7. Geben Sie im Feld **Benutzername** den Benutzernamen eines BES12-Benutzerkontos mit Administratorrechten ein.
8. Geben Sie im Feld **Kennwort** das Kennwort für das Konto ein.
9. Wählen Sie in der Dropdown-Liste **Verzeichnis** eine Authentifizierungsmethode aus.
10. Geben Sie, falls erforderlich, im Feld **Domäne** die Microsoft Active Directory-Domäne an.
11. Klicken Sie auf **Anmelden**.

Aktivieren von BlackBerry 10-Geräten mit dem BlackBerry Wired Activation Tool

Bevor Sie beginnen:

- Konfigurieren Sie das BlackBerry Wired Activation Tool, und melden Sie sich bei einer BES12-Instanz an.
- Schalten Sie alle verbundenen Geräte ein, und vergewissern Sie sich, dass bei allen Geräten die Ersteinrichtung abgeschlossen oder noch nicht begonnen wurde. Sie können keine Geräte aktivieren, wenn die Ersteinrichtung im Gang ist.

1. Verbinden Sie ein oder mehrere BlackBerry 10-Geräte mit USB-Kabeln mit Ihrem Computer.
2. Überprüfen Sie die Spalte **Status** für jedes Gerät. Führen Sie eine der folgenden Aktionen aus:
    - Wenn in der Spalte „Status“ **Kennwort erforderlich** angezeigt wird, klicken Sie auf **Kennwort erforderlich**, um das Kennwort für das Gerät einzugeben.
    - Wenn Sie in der Spalte „Status“ **Nicht unterstütztes Gerät** angezeigt wird, aktualisieren Sie die Gerätesoftware auf BlackBerry 10 OS Version 10.3 oder höher.
    - Wenn die Spalte „Status“ **Bereit** anzeigt wird, weisen Sie das Gerät einem Benutzer zu.
3. Suchen Sie mithilfe des Felds **Suchen** das Benutzerkonto, dem Sie das Gerät zuweisen möchten.
4. Klicken Sie im Suchergebnis auf das Benutzerkonto.
5. Klicken Sie im Hauptbereich des Bildschirms auf den Namen eines Benutzerkontos, und ziehen Sie den Namen auf ein Gerät, um dieses dem Benutzer zuzuweisen. Wiederholen Sie diesen Schritt, um weitere Geräte Benutzern zuzuweisen.
6. Aktivieren Sie die Kontrollkästchen neben den Benutzer-/Gerätepaaren, die Sie aktivieren möchten.
7. Klicken Sie auf **Geräte aktivieren**.

Das BlackBerry Wired Activation Tool aktiviert alle ausgewählten Geräte. Prüfen Sie die Spalte „Status“ auf Fortschritt und Ergebnis für die einzelnen Geräte. Wird eine Aktivierung nicht durchgeführt, klicken Sie auf die Meldung in der Spalte „Status“, um weitere Informationen zu Fehlern aufzurufen.

Tipps zur Fehlersuche bei der Geräteaktivierung

Zur Fehlersuche bei der Aktivierung von Geräten jeden Typs überprüfen Sie stets Folgendes:

- Vergewissern Sie sich, dass das Gerät von BES12 unterstützt wird. Informationen zu den unterstützten Gerätetypen finden Sie in der Kompatibilitätsmatrix.
- Vergewissern Sie sich, dass für den Gerätetyp, den der Benutzer aktiviert, und für die dem Benutzer zugewiesene Aktivierungsart Lizenzen verfügbar sind. Weitere Informationen finden Sie in der Dokumentation zur Lizenzierung.
- Überprüfen Sie die Netzwerkverbindung auf dem Gerät.
    - Stellen Sie sicher, dass das Mobilfunknetz bzw. das Wi-Fi-Netzwerk aktiv ist und ausreichender Empfang gegeben ist.
    - Wenn ein Benutzer manuell ein VPN-Profil oder ein geschäftliches Wi-Fi-Profil konfigurieren muss, um auf Inhalte hinter der Firewall Ihres Unternehmens zugreifen zu können, vergewissern Sie sich, dass die Profile auf dem Gerät richtig konfiguriert sind.
    - Wird das geschäftliche Wi-Fi verwendet, vergewissern Sie sich, dass der Gerätenetzwerkpfad verfügbar ist. Weitere Informationen zum Konfigurieren von Firewalls für BES12 finden Sie im Artikel KB36470 unter http://www.blackberry.com/btsc/.
- Stellen Sie sicher, dass das dem Benutzer zugewiesene Aktivierungsprofil eine Aktivierung des Gerätetyps zulässt.
- Wenn das Gerät versucht, eine Verbindung mit BES12 oder der BlackBerry Infrastructure über die Firewall des Unternehmens herzustellen, vergewissern Sie sich, dass die richtigen Firewall-Ports geöffnet sind. Informationen zu den erforderlichen Ports finden Sie in der Dokumentation zur Konfiguration.
- Sammeln Sie Geräteprotokolle:
    - Informationen zum Abrufen von BlackBerry 10-Protokolldateien finden Sie in Artikel KB26038 unter http://www.blackberry.com/btsc/.

      Hinweis: BlackBerry 10-Geräteprotokolldateien sind verschlüsselt. Zum Verwenden von BlackBerry 10-Geräteprotokolldateien für die Fehlerbehebung benötigen Sie ein offenes Ticket bei BlackBerry Technical Support Services. Nur Support-Mitarbeiter können die Protokolldateien entschlüsseln.
    - Informationen zum Abrufen von iOS-Protokolldateien finden Sie in Artikel KB36986 unter http://www.blackberry.com/btsc/.
    - Informationen zum Abrufen von Android-Protokolldateien finden Sie in Artikel KB32516 unter http://www.blackberry.com/btsc/.
    - Informationen zum Abrufen von Windows Phone-Protokollen finden Sie in Artikel KB36984 unter http://www.blackberry.com/btsc/.

KNOX Workspace und Android for Work

Zur Fehlersuche bei der Aktivierung von Samsung-Geräten mit Samsung KNOX Workspace überprüfen Sie Folgendes:

- Vergewissern Sie sich, dass das Gerät KNOX Workspace unterstützt. Weitere Informationen finden Sie auf der Webseite zu von Samsung KNOX unterstützten Geräten unter https://www.samsungknox.com/en/products/knox-supported-devices/knox-workspace.
- Vergewissern Sie sich, dass das Garantie-Bit nicht ausgelöst wurde. Weitere Informationen finden Sie im Artikel zu KNOX-Garantie-Bits und deren Auslösung unter https://www.samsungknox.com/en/faq/what-knox-warranty-bit-and-how-it-triggered
- Stellen Sie sicher, dass die KNOX-Containerversion unterstützt wird. KNOX Workspace erfordert KNOXContainer 2.0 oder höher. Weitere Informationen zu unterstützten Samsung KNOX-Versionen finden Sie unter https://www.samsungknox.com/knoxportal/files/GalaxyDevicesSupportingKNOX.pdf.

Zur Fehlersuche bei der Aktivierung von Android for Work-Geräten überprüfen Sie Folgendes:

- Vergewissern Sie sich, dass das Gerät Android for Work unterstützt. Weitere Informationen finden Sie in Artikel 6174145 unter https://support.google.com/work/android/answer/6174145.
- Stellen Sie sicher, dass eine Lizenz verfügbar und die Aktivierungsart auf „Geschäftlich und persönlich – Benutzer-Datenschutz (Android for Work)“ festgelegt ist.
- Zur Verwendung der Aktivierungsart „Geschäftlich und persönlich – Benutzer-Datenschutz (Android for Work)“ muss auf den Geräten Android Version 5.0 (Lollipop) oder höher ausgeführt werden.
- Vergewissern Sie sich, dass für das Benutzerkonto in BES12 die gleiche E-Mail-Adresse konfiguriert ist, wie für das in der Google-Domäne. Wenn die E-Mail-Adressen nicht übereinstimmen, wird auf dem Gerät gemeldet, dass es aufgrund einer nicht unterstützten Aktivierungsart nicht aktiviert werden kann. Suchen Sie in der Core-Protokolldatei nach folgenden Fehlern:
  - ```
    ERROR AfW: Could not find user in Google domain. Aborting user creation and activation.
    ```
  - ```
    ERROR job marked for quarantine due to: Unable to activate device - Unsupported activation type
    ```

Die Geräteaktivierung kann nicht abgeschlossen werden, da der Server keine Lizenzen hat. Wenden Sie sich bitte an Ihren Administrator.

Beschreibung

Dieser Fehler wird während der Aktivierung auf dem Gerät angezeigt, wenn keine Lizenzen zur Verfügung stehen oder die Lizenzen ausgelaufen sind.

Mögliche Lösung

Führen Sie in BES12 folgende Aktionen aus:

- Überprüfen Sie, ob Lizenzen zur Verfügung stehen, um die Aktivierung zu unterstützen.
- Aktivieren Sie ggf. Lizenzen oder kaufen Sie zusätzliche Lizenzen.

Überprüfen Sie Ihren Benutzernamen und Ihr Kennwort, und versuchen Sie es erneut.

Beschreibung

Dieser Fehler wird während der Aktivierung auf einem Gerät angezeigt, wenn der Benutzer einen falschen Benutzernamen, ein falsches Kennwort oder beides eingegeben hat.

Mögliche Lösung

Geben Sie den korrekten Benutzernamen und das korrekte Kennwort ein.

Das Profil konnte nicht installiert werden. Das Zertifikat „AutoMDMCert.pfx“ konnte nicht importiert werden.

Beschreibung

Dieser Fehler wird während der Aktivierung auf einem iOS-Gerät angezeigt, wenn bereits ein Profil auf dem Gerät vorhanden ist.

Mögliche Lösung

Wechseln Sie auf dem Gerät zu **Einstellungen** > **Allgemeine Einstellungen** > **Profil**, und überprüfen Sie, ob bereits ein Profil vorhanden ist. Entfernen Sie das vorhandene Profil, und aktivieren Sie das gewünschte Profil erneut. Wenn der Fehler weiterhin besteht, müssen Sie das Gerät möglicherweise zurücksetzen, da eventuell Daten zwischengespeichert wurden.

Fehler 3007: Server nicht verfügbar

Beschreibung

Dieser Fehler wird während der Aktivierung auf dem Gerät angezeigt, wenn das von BES12 verwendete SSL-Zertifikat dem iOS-Gerät nicht vertrauenswürdig erscheint.

Mögliche Lösung

Das Zertifizierungsstellenzertifikat des Servers, das zum Erstellen des SSL-Zertifikats für BES12 verwendet wurde, muss auf dem iOS-Gerät installiert sein.

Serververbindung konnte nicht hergestellt werden, bitte überprüfen Sie die Konnektivität und die Serveradresse

Beschreibung

Dieser Fehler kann aus folgenden Gründen während der Aktivierung auf dem Gerät auftreten:

- Der Benutzername wurde fehlerhaft auf dem Gerät eingegeben.
- Die Kundenadresse für die Geräteaktivierung wurde fehlerhaft auf dem Gerät eingegeben.

  Hinweis: Dies ist nur erforderlich, wenn die Registrierung bei der BlackBerry Infrastructure deaktiviert wurde.
- Es wurde kein Aktivierungskennwort gesetzt, oder das Kennwort ist abgelaufen.

Mögliche Lösungen

Lösungsmöglichkeiten:

- Überprüfen Sie den Benutzernamen und das Kennwort.
- Überprüfen Sie die Kundenadresse für die Geräteaktivierung.
- Setzen Sie mithilfe von BES12 Self-Service ein neues Aktivierungskennwort.

iOS-Geräteaktivierungen schlagen bei ungültigen APNs-Zertifikaten fehl.

Problemursache

Wenn Sie iOS-Geräte nicht aktivieren können, wurde das APNs-Zertifikat möglicherweise nicht ordnungsgemäß registriert.

Mögliche Lösung

Führen Sie eine oder mehrere der folgenden Aktionen aus:

- Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen** > **Externe Integration** > **iOS-Verwaltung**. Vergewissern Sie sich, dass das APNs-Zertifikat den Status „Installiert“ aufweist. Wenn der Status nicht korrekt ist, versuchen Sie, das APNs-Zertifikat erneut zu registrieren.
- Zum Testen der Verbindung zwischen BES12 und dem APNs-Server klicken Sie auf **APNS-Zertifikat testen**.
- Rufen Sie ggf. eine neue signierte CSR von BlackBerry ab, fordern Sie ein neues APNs-Zertifikat an, und registrieren Sie es.

Die Benutzer erhalten keine Aktivierungs-E-Mail

Beschreibung

Die Benutzer erhalten ihre Aktivierungs-E-Mail nicht, obwohl alle Einstellungen in BES12 korrekt sind.

Mögliche Lösung

Wenn Sie den Mailserver eines Drittanbieters nutzen, werden E-Mail-Nachrichten von BES12 eventuell als Spam markiert und in den Spam-E-Mail-Ordner oder den Junk-E-Mail-Ordner verschoben.

Überprüfen Sie, ob die Benutzer in Ihrem Spam-E-Mail-Ordner und dem Junk-E-Mail-Ordner nach der Aktivierungs-E-Mail gesucht haben.

Verwalten von Geräten

26

BES12 umfasst Befehle, die Sie über das drahtlose Netzwerk an Geräte senden können, um Daten auf den Geräten zu schützen. Sie können detaillierte Informationen zu einzelnen Geräten in Geräteberichten anzeigen.

Verwenden von Dashboard-Berichten

Das Dashboard präsentiert die systemeigenen Benutzer- und Geräteinformationen aus den BES12-Diensten in Form von Graphiken. Wenn Sie den Cursor über einen Datenpunkt bewegen (z. B. über ein Segment in einem Kreisdiagramm) können Sie Informationen zu den Benutzern oder Geräten anzeigen.

Wenn Sie weitere Informationen benötigen, können Sie einen Bericht aus der Graphik aufrufen, um detaillierte Informationen zu den Benutzern oder Geräten anzuzeigen. Die maximale Anzahl an Einträgen in einem Bericht ist auf 2000 begrenzt. Sie können aus dem Bericht eine .csv Datei erstellen und die Datei zu weiteren Analyse- oder Reporting-Zwecken exportieren.

Um ein Benutzerkonto zu öffnen und zu verwalten, können Sie in einem Bericht auf den Benutzer oder das Gerät klicken. Wenn Sie ein Konto abgeschlossen haben, können Sie auf der Seite (nicht im Browser) durch Klicken auf „Zurück“ wieder zum Bericht zurückkehren.

In der folgenden Tabelle werden die Informationen beschrieben, die jeder einzelne Dashboard-Bericht anzeigt.

Dashboard-Bericht	Beschreibung
Geräte mit und ohne Roaming	Eine Liste der Benutzer mit Geräten, die sich derzeit in einem Roaming-Status befinden
Geräteaktivierungen	Eine dynamische Darstellung der Geräte, die im Laufe einer 12-monatigen Phase pro Monat in Ihrer Organisation aktiviert wurden. Die Informationen basieren auf dem Zeitpunkt, an dem die Geräte erstmalig aktiviert wurden. Die Anzahl der Geräte ändert sich und spiegelt so die derzeit aktivierten Geräte wieder. Beispiel: Wird ein Gerät deaktiviert, das Sie im August aktiviert haben, wird die im August dargestellte Anzahl der Geräte um ein Gerät reduziert.
Fünf verwaltete, am häufigsten installierte Apps	Die fünf häufigsten Apps, die von Ihrer Organisation zugewiesen und auf Geräten installiert wurden
Geräte nach Plattform	Eine Liste der in Ihrer Organisation vorhandenen Geräte, geordnet nach der Plattform
Gerätekompatibilität	Eine Liste der Probleme, die bei BlackBerry 10-, iOS-, Android- und Windows Phone-Geräten in Ihrer Organisation erkannt wurden
Geräte, geordnet nach dem letzten Kontaktzeitpunkt	Die Anzahl der Tage, die seit der letzten Kontaktaufnahme der Geräte mit dem Server vergangen sind
Geräte nach Betreiber	Eine Liste der Geräte in Ihrer Organisation, geordnet nach Dienstanbieter

Dashboard-Bericht	Beschreibung
Die fünf häufigsten Mobilgeräte	Die fünf häufigsten Mobilgerät-Modelle in Ihrer Organisation

Ändern des Grafiktyps

Sie können den Grafiktyp ändern, der zur graphischen Darstellung von Informationen verwendet wird.

Klicken Sie neben einer Grafik auf ⚙, und wählen Sie aus der Dropdown-Liste einen Grafiktyp aus.

Exportieren eines Dashboard-Berichts in eine .csv-Datei

1. Um einen Bericht zu öffnen, klicken Sie auf eine Graphik.
2. Um die Einträge anhand der ausgewählten Spalte zu sortieren, klicken Sie auf eine Spaltenüberschrift.
3. Klicken Sie auf **Exportieren**, und speichern Sie die Datei.

Verwenden von IT-Administrationsbefehlen zum Verwalten von Geräten

Sie können verschiedene IT-Administrationsbefehle über das Mobilfunknetz senden, sodass Sie Geräte per Fernzugriff verwalten können.

Sie können IT-Administrationsbefehle beispielweise unter folgenden Umständen verwenden:

- Wenn ein Gerät vorübergehend verlegt wurde, können Sie einen Befehl zum Sperren des Geräts senden oder geschäftliche Daten auf dem Gerät löschen.
- Wenn Sie ein Gerät einem anderen Benutzer in Ihrem Unternehmen zuteilen möchten oder wenn ein Gerät verloren gegangen ist oder gestohlen wurde, können Sie einen Befehl senden, um alle Daten auf dem Gerät zu löschen.
- Wenn ein Mitarbeiter aus Ihrem Unternehmen ausscheidet, können Sie einen Befehl an das persönliche Gerät des Benutzers senden, um ausschließlich die geschäftlichen Daten zu löschen.
- Wenn ein Benutzer das Kennwort für den geschäftlichen Bereich vergisst, können Sie einen Befehl senden, um dieses Kennwort zurückzusetzen.

Die Liste der verfügbaren IT-Administrationsbefehle hängt vom Gerätetyp und von der Aktivierungsart ab.

Senden eines IT-Administrationsbefehls an ein Gerät

Sie können verschiedene Befehle über das drahtlose Netzwerk an ein Gerät senden.

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte**.

2. Suchen Sie nach einem Benutzerkonto.
3. Klicken Sie in den Suchergebnissen auf den Namen des Benutzerkontos.
4. Klicken Sie auf die Registerkarte „Gerät“.
5. Wählen Sie im Fenster **Gerät verwalten** den Befehl aus, den Sie an das Gerät senden möchten.

IT-Administrationsbefehle

In den folgenden Tabellen werden die verfügbaren IT-Administrationsbefehle nach Gerätetyp aufgeführt.

BlackBerry 10

IT-Administrations-befehl	Beschreibung	Aktivierungsarten
Gerätekennwort festlegen, Gerät sperren und Nachricht einrichten	Mit diesem Befehl erstellen Sie ein Gerätekennwort und legen eine Nachricht fest, die auf dem Startbildschirm angezeigt wird. Anschließend wird das Gerät gesperrt. Sie müssen ein Kennwort erstellen, das die bestehenden Kennwortregeln erfüllt. Wenn der Benutzer das Gerät entsperrt, wird er vom Gerät aufgefordert, das neue Kennwort zu akzeptieren oder abzulehnen. Wenn eine IT-Richtlinie erfordert, dass das Gerät das gleiche Kennwort für das Gerät und den geschäftlichen Bereich nutzen muss, ändert dieser Befehl zudem das Kennwort für den geschäftlichen Bereich.	• Geschäftlich und persönlich – Unternehmen • Nur geschäftlicher Bereich • Geschäftlich und persönlich – Reguliert
Alle Gerätedaten löschen	Mit diesem Befehl werden alle Benutzerinformationen und App-Daten gelöscht, die auf dem Gerät gespeichert sind, einschließlich der im geschäftlichen Bereich. Er setzt das Gerät auf die werkseitigen Standardeinstellungen zurück und löscht das Gerät optional aus BES12. Nachdem Sie diesen Befehl gesendet haben, können Sie das Gerät optional aus BES12 löschen. Wenn das Gerät keine Verbindung zu BES12 herstellen kann, können Sie das Gerät aus BES12 löschen. Wenn das Gerät eine Verbindung zu BES12 herstellt, nachdem es gelöscht wurde, werden nur die geschäftlichen Daten vom Gerät entfernt. Falls zutreffend, wird auch der geschäftliche Bereich entfernt.	• Geschäftlich und persönlich – Unternehmen • Nur geschäftlicher Bereich • Geschäftlich und persönlich – Reguliert
Kennwort für den geschäftlichen	Mit diesem Befehl können Sie ein neues Kennwort für den geschäftlichen Bereich auf dem Gerät festlegen und den geschäftlichen Bereich sperren. Sie müssen ein Kennwort	• Geschäftlich und persönlich – Unternehmen

IT-Administrations-befehl	Beschreibung	Aktivierungsarten
Bereich festlegen und diesen sperren	erstellen, das die bestehenden Kennwortregeln erfüllt. Um den geschäftlichen Bereich zu entsperren, muss der Benutzer das neue von Ihnen erstellte Kennwort eingeben. Wenn eine IT-Richtlinie erfordert, dass das Gerät das gleiche Kennwort für das Gerät und den geschäftlichen Bereich nutzen muss, ändert dieser Befehl zudem das Gerätekennwort.	• Geschäftlich und persönlich – Reguliert
Nur Geschäftsdaten löschen	Mit diesem Befehl werden geschäftliche Daten, einschließlich der auf dem Gerät vorhandenen IT-Richtlinie, Profile, Apps und Zertifikate, gelöscht und das Gerät optional aus BES12 entfernt. Wenn das Gerät über einen geschäftlichen Bereich verfügt, werden die Informationen im geschäftlichen Bereich sowie der Bereich selbst aus dem Gerät gelöscht. Durch Senden dieses Befehls wird das Benutzerkonto nicht gelöscht. Nachdem Sie diesen Befehl gesendet haben, können Sie das Gerät optional aus BES12 löschen. Wenn das Gerät keine Verbindung zu BES12 herstellen kann, können Sie das Gerät aus BES12 löschen. Wenn das Gerät eine Verbindung zu BES12 herstellt, nachdem es gelöscht wurde, werden nur die geschäftlichen Daten vom Gerät entfernt. Falls zutreffend, wird auch der geschäftliche Bereich entfernt.	• Geschäftlich und persönlich – Unternehmen • Geschäftlich und persönlich – Reguliert
Geräteinformationen aktualisieren	Dieser Befehl sendet und empfängt aktualisierte Gerätedaten. Beispielsweise können Sie kürzlich aktualisierte IT-Richtlinienregeln oder Profile an ein Gerät senden und aktualisierte Informationen zu einem Gerät, wie Betriebssystemversion oder Akkuladezustand, empfangen.	• Geschäftlich und persönlich – Unternehmen • Nur geschäftlicher Bereich • Geschäftlich und persönlich – Reguliert

BlackBerry OS (Version 5.0 bis 7.1)

IT-Administrations-befehl	Beschreibung
Gerätekennwort festlegen und sperren	Mit diesem Befehl erstellen Sie ein Gerätekennwort. Anschließend wird das Gerät gesperrt. Sie müssen ein Kennwort erstellen, das die bestehenden Kennwortregeln erfüllt. Wenn Sie oder ein

IT-Administrations-befehl	Beschreibung
	Benutzer den Zwei-Faktor-Inhaltsschutz eingeschaltet haben, können Sie diesen Befehl nicht verwenden.
Nur Geschäftsdaten löschen	Mit diesem Befehl werden geschäftliche Daten, einschließlich der IT-Richtlinie, E-Mail-Nachrichten, Kontakte und geschäftlichen Servicebücher gelöscht. Alle persönlichen Daten bleiben auf dem Gerät erhalten.
Alle Gerätedaten löschen	Mit diesem Befehl werden alle Benutzerinformationen und App-Daten gelöscht, die auf dem Gerät gespeichert sind. Außerdem wird das Gerät auf die werkseitigen Standardeinstellungen zurückgesetzt. Sie können diesen Befehl an ein Gerät, das Sie einem anderen Benutzer zuteilen möchten, oder an ein Gerät, das verloren gegangen ist und das der Benutzer möglicherweise nicht wiederfindet, senden.
Servicebücher erneut senden	Dieser Befehl sendet Servicebücher erneut an ein Gerät. Servicebücher legen fest, welche Dienste auf einem BlackBerry OS-Gerät verfügbar sind.
IT-Richtlinie erneut senden	Dieser Befehl sendet die zugewiesene BlackBerry OS-IT-Richtlinie erneut an ein Gerät.

iOS

IT-Administrations-befehl	Beschreibung	Aktivierungsarten
Alle Gerätedaten löschen	Mit diesem Befehl werden alle Benutzerinformationen und App-Daten gelöscht, die auf dem Gerät gespeichert sind, einschließlich der im geschäftlichen Bereich. Er setzt das Gerät auf die werkseitigen Standardeinstellungen zurück und löscht das Gerät optional aus BES12. Nachdem Sie diesen Befehl gesendet haben, können Sie das Gerät optional aus BES12 löschen. Wenn das Gerät keine Verbindung zu BES12 herstellen kann, können Sie das Gerät aus BES12 löschen. Wenn das Gerät eine Verbindung zu BES12 herstellt, nachdem es gelöscht wurde, werden nur die geschäftlichen Daten vom Gerät entfernt. Falls zutreffend, wird auch der geschäftliche Bereich entfernt.	• MDM-Steuerelemente • Geschäftlich und persönlich – vollständige Kontrolle
Nur Geschäftsdaten löschen	Mit diesem Befehl werden geschäftliche Daten, einschließlich der auf dem Gerät vorhandenen IT-Richtlinie, Profile, Apps und Zertifikate, gelöscht und das Gerät optional aus BES12 entfernt.	• MDM-Steuerelemente • Geschäftlich und persönlich – vollständige Kontrolle

IT-Administrations-befehl	Beschreibung	Aktivierungsarten
	Wenn das Gerät über einen geschäftlichen Bereich verfügt, werden die Informationen im geschäftlichen Bereich sowie der Bereich selbst aus dem Gerät gelöscht. Durch Senden dieses Befehls wird das Benutzerkonto nicht gelöscht. Nachdem Sie diesen Befehl gesendet haben, können Sie das Gerät optional aus BES12 löschen. Wenn das Gerät keine Verbindung zu BES12 herstellen kann, können Sie das Gerät aus BES12 löschen. Wenn das Gerät eine Verbindung zu BES12 herstellt, nachdem es gelöscht wurde, werden nur die geschäftlichen Daten vom Gerät entfernt. Falls zutreffend, wird auch der geschäftliche Bereich entfernt.	• Geschäftlich und persönlich – Benutzer-Datenschutz
Gerät sperren	Mit diesem Befehl sperren Sie ein Gerät. Der Benutzer muss das bestehende Gerätekennwort eingeben, um das Gerät zu entsperren. Wenn ein Gerät vorübergehend verlegt wurde, können Sie diesen Befehl verwenden. Wenn Sie diesen Befehl senden, wird das Gerät nur gesperrt, wenn ein Gerätekennwort vorhanden ist. Andernfalls wird auf dem Gerät keine Aktion ausgeführt.	• MDM-Steuerelemente • Geschäftlich und persönlich – vollständige Kontrolle
Entsperren und Kennwort löschen	Dieser Befehl entsperrt ein Gerät und löscht das bestehende Kennwort. Der Benutzer wird zur Eingabe eines Gerätekennworts aufgefordert. Sie können diesen Befehl verwenden, wenn der Benutzer das Gerätekennwort vergessen hat.	• MDM-Steuerelemente • Geschäftlich und persönlich – vollständige Kontrolle
Geschäftlichen Bereich sperren	Dieser Befehl sperrt den geschäftlichen Bereich auf einem Gerät, sodass der Benutzer das bestehende Kennwort für den geschäftlichen Bereich eingeben muss, um das Gerät zu entsperren.	• Geschäftlich und persönlich – vollständige Kontrolle • Geschäftlich und persönlich – Benutzer-Datenschutz
Kennwort für geschäftlichen Bereich zurücksetzen	Dieser Befehl löscht das aktuelle Kennwort für den geschäftlichen Bereich vom Gerät. Wenn der Benutzer den geschäftlichen Bereich öffnet, fordert das Gerät ihn auf, ein neues Kennwort für den geschäftlichen Bereich festzulegen.	• Geschäftlich und persönlich – vollständige Kontrolle • Geschäftlich und persönlich – Benutzer-Datenschutz

IT-Administrations-befehl	Beschreibung	Aktivierungsarten
Geschäftlichen Bereich aktivieren/ deaktivieren	Dieser Befehl aktiviert bzw. deaktiviert den Zugriff auf die Apps für den geschäftlichen Bereich auf dem Gerät.	• Geschäftlich und persönlich – vollständige Kontrolle • Geschäftlich und persönlich – Benutzer-Datenschutz
Gerätedaten aktualisieren	Dieser Befehl sendet und empfängt aktualisierte Gerätedaten. Beispielsweise können Sie kürzlich aktualisierte IT-Richtlinienregeln oder Profile an ein Gerät senden und aktualisierte Informationen zu einem Gerät, wie Betriebssystemversion oder Akkuladezustand, empfangen.	• MDM-Steuerelemente • Geschäftlich und persönlich – vollständige Kontrolle

Android

IT-Administrations-befehl	Beschreibung	Aktivierungsarten
Alle Gerätedaten löschen	Mit diesem Befehl werden alle Benutzerinformationen und App-Daten gelöscht, die auf dem Gerät gespeichert sind, einschließlich der im geschäftlichen Bereich. Er setzt das Gerät auf die werkseitigen Standardeinstellungen zurück und löscht das Gerät optional aus BES12. Nachdem Sie diesen Befehl gesendet haben, können Sie das Gerät optional aus BES12 löschen. Wenn das Gerät keine Verbindung zu BES12 herstellen kann, können Sie das Gerät aus BES12 löschen. Wenn das Gerät eine Verbindung zu BES12 herstellt, nachdem es gelöscht wurde, werden nur die geschäftlichen Daten vom Gerät entfernt. Falls zutreffend, wird auch der geschäftliche Bereich entfernt.	• MDM-Steuerelemente • Geschäftlich und persönlich – vollständige Kontrolle (Secure Work Space) • Geschäftlich und persönlich – vollständige Kontrolle (Samsung KNOX) • Nur geschäftlicher Bereich - (Samsung KNOX)
Nur Geschäftsdaten löschen	Mit diesem Befehl werden geschäftliche Daten, einschließlich der auf dem Gerät vorhandenen IT-Richtlinie, Profile, Apps und Zertifikate, gelöscht und das Gerät optional aus BES12 entfernt. Wenn das Gerät über einen geschäftlichen Bereich verfügt, werden die Informationen im geschäftlichen Bereich sowie der Bereich selbst aus dem Gerät gelöscht. Durch Senden dieses Befehls wird das Benutzerkonto nicht gelöscht.	• MDM-Steuerelemente • Geschäftlich und persönlich – Benutzer-Datenschutz (Secure Work Space) • Geschäftlich und persönlich – vollständige Kontrolle (Secure Work Space)

IT-Administrations-befehl	Beschreibung	Aktivierungsarten
	Nachdem Sie diesen Befehl gesendet haben, können Sie das Gerät optional aus BES12 löschen. Wenn das Gerät keine Verbindung zu BES12 herstellen kann, können Sie das Gerät aus BES12 löschen. Wenn das Gerät eine Verbindung zu BES12 herstellt, nachdem es gelöscht wurde, werden nur die geschäftlichen Daten vom Gerät entfernt. Falls zutreffend, wird auch der geschäftliche Bereich entfernt.	• Geschäftlich und persönlich – vollständige Kontrolle (Samsung KNOX) • Nur geschäftlicher Bereich - (Samsung KNOX) • Geschäftlich und persönlich – Benutzer-Datenschutz (Android for Work) • Geschäftlich und persönlich – Benutzer-Datenschutz (Android for Work - Premium)
Gerät sperren	Mit diesem Befehl sperren Sie ein Gerät. Der Benutzer muss das bestehende Gerätekennwort eingeben, um das Gerät zu entsperren. Wenn ein Gerät vorübergehend verlegt wurde, können Sie diesen Befehl verwenden. Wenn Sie diesen Befehl senden, wird das Gerät nur gesperrt, wenn ein Gerätekennwort vorhanden ist. Andernfalls wird auf dem Gerät keine Aktion ausgeführt.	• MDM-Steuerelemente • Geschäftlich und persönlich – vollständige Kontrolle (Secure Work Space) • Geschäftlich und persönlich – vollständige Kontrolle (Samsung KNOX) • Geschäftlich und persönlich – Benutzer-Datenschutz (Android for Work) • Geschäftlich und persönlich – Benutzer-Datenschutz (Android for Work - Premium)
Entsperren und Kennwort löschen	Dieser Befehl entsperrt ein Gerät und löscht das bestehende Kennwort. Der Benutzer wird zur Eingabe eines Gerätekennworts aufgefordert. Sie können diesen Befehl verwenden, wenn der Benutzer das Gerätekennwort vergessen hat.	• MDM-Steuerelemente • Geschäftlich und persönlich – vollständige Kontrolle (Secure Work Space) • Geschäftlich und persönlich – vollständige Kontrolle (Samsung KNOX)
Geschäftlichen Bereich sperren	Dieser Befehl sperrt den geschäftlichen Bereich auf einem Gerät, sodass der Benutzer das bestehende Kennwort für den	• Geschäftlich und persönlich – vollständige Kontrolle (Secure Work Space)

IT-Administrations-befehl	Beschreibung	Aktivierungsarten
	geschäftlichen Bereich eingeben muss, um das Gerät zu entsperren.	• Geschäftlich und persönlich – Benutzer-Datenschutz (Secure Work Space)
Kennwort für geschäftlichen Bereich zurücksetzen	Dieser Befehl löscht das aktuelle Kennwort für den geschäftlichen Bereich vom Gerät. Wenn der Benutzer den geschäftlichen Bereich öffnet, fordert das Gerät ihn auf, ein neues Kennwort für den geschäftlichen Bereich festzulegen.	• Geschäftlich und persönlich – vollständige Kontrolle (Secure Work Space) • Geschäftlich und persönlich – Benutzer-Datenschutz (Secure Work Space) • Geschäftlich und persönlich – vollständige Kontrolle (Samsung KNOX) • Nur geschäftlicher Bereich - (Samsung KNOX)
Geschäftlichen Bereich aktivieren/ deaktivieren	Dieser Befehl aktiviert bzw. deaktiviert den Zugriff auf die Apps für den geschäftlichen Bereich auf dem Gerät.	• Geschäftlich und persönlich – vollständige Kontrolle (Secure Work Space) • Geschäftlich und persönlich – Benutzer-Datenschutz (Secure Work Space) • Geschäftlich und persönlich – vollständige Kontrolle (Samsung KNOX) • Nur geschäftlicher Bereich - (Samsung KNOX)
Gerätekennwort festlegen und sperren	Mit diesem Befehl erstellen Sie ein Gerätekennwort. Anschließend wird das Gerät gesperrt. Sie müssen ein Kennwort erstellen, das die bestehenden Kennwortregeln erfüllt. Wenn der Benutzer das Gerät entsperrt, wird er vom Gerät aufgefordert, das neue Kennwort zu akzeptieren oder abzulehnen.	• MDM-Steuerelemente • Geschäftlich und persönlich – vollständige Kontrolle (Secure Work Space) • Geschäftlich und persönlich – vollständige Kontrolle (Samsung KNOX)

IT-Administrations-befehl	Beschreibung	Aktivierungsarten
Geräteinformationen aktualisieren	Dieser Befehl sendet und empfängt aktualisierte Gerätedaten. Beispielsweise können Sie kürzlich aktualisierte IT-Richtlinienregeln oder Profile an ein Gerät senden und aktualisierte Informationen zu einem Gerät, wie Betriebssystemversion oder Akkuladezustand, empfangen.	• MDM-Steuerelemente • Geschäftlich und persönlich – vollständige Kontrolle (Secure Work Space) • Geschäftlich und persönlich – vollständige Kontrolle (Samsung KNOX) • Nur geschäftlicher Bereich - (Samsung KNOX) • Geschäftlich und persönlich – Benutzer-Datenschutz (Android for Work) • Geschäftlich und persönlich – Benutzer-Datenschutz (Android for Work - Premium)

Windows Phone

IT-Administrations-befehl	Beschreibung	Aktivierungsarten
Gerät sperren	Mit diesem Befehl sperren Sie ein Gerät. Der Benutzer muss das bestehende Gerätekennwort eingeben, um das Gerät zu entsperren. Wenn ein Gerät vorübergehend verlegt wurde, können Sie diesen Befehl verwenden. Wenn Sie diesen Befehl senden, wird das Gerät nur gesperrt, wenn ein Gerätekennwort vorhanden ist. Andernfalls wird auf dem Gerät keine Aktion ausgeführt. Dieser Befehl wird auf Geräten, auf denen Windows Phone 8.1 oder höher ausgeführt wird, unterstützt.	MDM-Steuerelemente
Gerätekennwort erstellen und Gerät sperren	Mit diesem Befehl wird ein neues Kennwort generiert und das Gerät gesperrt. Das generierte Kennwort wird dem Benutzer per E-Mail gesendet. Sie können die vorgewählte E-Mail-Adresse verwenden oder eine E-Mail-Adresse angeben. Das generierte Kennwort erfüllt alle bestehenden Kennwortregeln.	MDM-Steuerelemente

IT-Administrations-befehl	Beschreibung	Aktivierungsarten
	Dieser Befehl wird auf Geräten mit Windows Phone OS-Version 8.10.14176 oder höher unterstützt.	
Nur Geschäftsdaten löschen	Mit diesem Befehl werden geschäftliche Daten, einschließlich der auf dem Gerät vorhandenen IT-Richtlinie, Profile, Apps und Zertifikate, gelöscht und das Gerät optional aus BES12 entfernt. Durch Senden dieses Befehls wird das Benutzerkonto nicht gelöscht. Nachdem Sie diesen Befehl gesendet haben, können Sie das Gerät optional aus BES12 löschen. Wenn das Gerät keine Verbindung zu BES12 herstellen kann, können Sie das Gerät aus BES12 löschen. Wenn das Gerät eine Verbindung zu BES12 herstellt, nachdem es gelöscht wurde, werden nur die geschäftlichen Daten vom Gerät entfernt. Falls zutreffend, wird auch der geschäftliche Bereich entfernt.	MDM-Steuerelemente
Alle Gerätedaten löschen	Mit diesem Befehl werden alle Benutzerinformationen und App-Daten gelöscht, die auf dem Gerät gespeichert sind. Er setzt das Gerät auf die werkseitigen Standardeinstellungen zurück und löscht das Gerät optional aus BES12. Nachdem Sie diesen Befehl gesendet haben, können Sie das Gerät optional aus BES12 löschen. Wenn das Gerät keine Verbindung zu BES12 herstellen kann, können Sie das Gerät aus BES12 löschen. Wenn das Gerät eine Verbindung zu BES12 herstellt, nachdem es gelöscht wurde, werden nur die geschäftlichen Daten vom Gerät entfernt. Falls zutreffend, wird auch der geschäftliche Bereich entfernt.	MDM-Steuerelemente
Geräteinformationen aktualisieren	Dieser Befehl sendet und empfängt aktualisierte Gerätedaten. Beispielsweise können Sie kürzlich aktualisierte IT-Richtlinienregeln oder Profile an ein Gerät senden und aktualisierte Informationen zu einem Gerät, wie Betriebssystemversion oder Akkuladezustand, empfangen.	MDM-Steuerelemente

Anzeigen und Speichern eines Geräteberichts

Sie können einen Gerätebericht generieren, um detaillierte Informationen zu jedem Gerät, das mit BES12 verknüpft ist, anzuzeigen.

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte**.
2. Suchen Sie nach einem Benutzerkonto.
3. Klicken Sie in den Suchergebnissen auf den Namen des Benutzerkontos.
4. Klicken Sie auf die Registerkarte „Gerät“.
5. Klicken Sie auf **Anzeigen des Geräteberichts**.
6. Klicken Sie auf **Exportieren**, um den Gerätebericht ggf. in einer Datei auf dem Computer zu speichern.

Überprüfen, ob ein Gerät für den Zugriff auf geschäftliche E-Mails und Terminplanerdaten zugelassen ist

Wenn Ihre Organisation BlackBerry Gatekeeping Service verwendet, um zu steuern, welche Geräte von Exchange ActiveSync aus auf geschäftliche E-Mails und Terminplanerdaten zugreifen können, wird mindestens ein Gatekeeping-Server für ein E-Mail-Profil konfiguriert. Wenn das E-Mail-Profil mit konfiguriertem Gatekeeping einem Benutzerkonto zugewiesen wird, können Sie den Verbindungsstatus zwischen einem Gerät und Exchange ActiveSync überprüfen. Sie können den Status suchen, indem Sie sich die Seite mit den Gerätedetails im Abschnitt „IT-Richtlinien und -Profile“ ansehen. Die folgenden Statuswerte werden bei den Gerätedetails neben dem E-Mail-Profil angezeigt.

Status	Beschreibung
Unbekannt	Der Status „Unbekannt“ wird angezeigt, wenn BES12 die ID des Geräts nicht bestimmen kann. Das Gerät wird in der Liste der gesperrten Geräten aufgeführt und muss der zugelassenen Liste manuell hinzugefügt werden.
Anstehende Verbindung	Der Status „Anstehende Verbindung“ wird angezeigt, wenn BES12 die ID des Geräts kennt und das Gerät in der Warteschlange auf die Hinzufügung zur zugelassenen Liste wartet.
Zugelassene Verbindung	Der Status „Zugelassene Verbindung“ wird angezeigt, wenn BES12 die ID des Geräts kennt und das Gerät auf der zugelassenen Liste vorhanden ist.

Überprüfen, ob ein Gerät zugelassen ist

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte**.
2. Suchen Sie nach einem Benutzerkonto.
3. Klicken Sie in den Suchergebnissen auf den Namen eines Benutzerkontos.
4. Wählen Sie die Registerkarte für das zu überprüfende Gerät aus.

5. Wenn das Gerät zugelassen ist, wird im Abschnitt **IT-Richtlinien und -Profile** neben dem E-Mail-Profil **Verbindung zugelassen** angezeigt.

Exchange Gatekeeping

Wenn Ihre Organisation BlackBerry Gatekeeping Service verwendet, um zu steuern, welche Geräte auf Exchange ActiveSync zugreifen können, werden alle Geräte, die nicht auf der Positivliste für Microsoft Exchange stehen, auf der BES12-Liste mit gesperrten Exchange ActiveSync-Geräten gemeldet.

Wenn Sie ein Benutzerkonto hinzufügen und diesem ein E-Mail-Profil zuweisen, für das BlackBerry Gatekeeping Service konfiguriert ist, werden alle zuvor gesperrten, in Quarantäne befindlichen oder manuell zugelassenen Geräte im Zusammenhang mit dem Benutzerkonto auf der Liste der gesperrten Exchange ActiveSync-Geräte angezeigt.

Wenn BES12 keine Exchange ActiveSync-ID von einem Gerät abrufen kann, wird es für Microsoft Exchange nicht der zugelassenen Liste hinzugefügt. Sie können diese Geräte der zugelassenen Liste manuell aus der Liste der gesperrten Exchange ActiveSync-Geräten hinzufügen. Wenn ein Android-Gerät beispielsweise ohne Secure Work Space mithilfe der MDM-Aktivierungsart aktiviert wird, kann BES12 keine Exchange ActiveSync-ID abrufen, und Sie müssen das Gerät in der Liste der gesperrten Exchange ActiveSync-Geräte manuell der Positivliste hinzufügen.

Ermöglichen des Zugriffs eines Geräts auf Microsoft ActiveSync

Sie können den Zugriff eines Geräts auf Microsoft ActiveSync manuell ermöglichen, sodass Benutzer E-Mail-Nachrichten und andere Informationen vom Microsoft Exchange Server auf dem Gerät abrufen können.

Bevor Sie beginnen: Erstellen einer Microsoft Exchange-Konfiguration

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte**.
2. Klicken Sie auf **Exchange Gatekeeping**.
3. Suchen Sie ein Gerät.
4. Klicken Sie in der Spalte **Aktion** auf ✓.

Sperren eines Geräts für den Zugriff auf Microsoft ActiveSync

Sie können ein zuvor zugelassenes Geräte manuell vom Zugriff auf Microsoft ActiveSync ausschließen. Der Ausschluss eines Geräts verhindert, dass Benutzer E-Mail-Nachrichten und andere Informationen vom Microsoft Exchange Server auf dem Gerät abrufen.

Bevor Sie beginnen: Erstellen einer Microsoft Exchange-Konfiguration

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte**.
2. Klicken Sie auf **Exchange Gatekeeping**.
3. Suchen Sie ein Gerät.
4. Klicken Sie in der Spalte **Aktion** auf ⃠.

Deaktivieren von Geräten

Wenn Sie oder ein Benutzer ein Gerät deaktiviert, wird die Verbindung zwischen dem Gerät und dem Benutzerkonto in BES12 entfernt. Sie können das Gerät nicht verwalten, und das Gerät wird nicht in der Verwaltungskonsole angezeigt. Der Benutzer kann nicht auf die geschäftlichen Daten auf dem Gerät zugreifen.

Sie können ein Gerät mit dem Befehl „Nur Geschäftsdaten löschen“ deaktivieren.

Benutzer können ein iOS-, Android- oder Windows Phone-Gerät deaktivieren, indem sie „Mein Gerät deaktivieren“ auf dem Bildschirm „Info“ im BES12 Client auswählen.

Benutzer können den geschäftlichen Bereich auf einem BlackBerry 10-Gerät deaktivieren, indem sie „Einstellungen > BlackBerry Balance > Geschäftlichen Bereich löschen“ auswählen.

Wenn Android-Geräte, die KNOX MDM verwenden, deaktiviert werden, werden interne Apps deinstalliert, und die Option „Deinstallieren“ wird für beliebige öffentliche Apps, die von der Apps-Liste aus installiert wurden, nach Bedarf verfügbar.

Bestimmen des Standorts von iOS-Geräten

Sie können die aktuellen Standorte von bis zu 100 iOS-Geräten auf einer Karte in der Verwaltungskonsole anzeigen und Benutzern ermöglichen, ihr eigenes iOS-Gerät auf einer Karte in BES12 Self-Service anzuzeigen. Sie können Benutzern, Benutzergruppen und Gerätegruppen ein Profil für die Standortbestimmung zuweisen. Sie können iOS-Geräte orten, die verloren oder gestohlen wurden.

Sie müssen benötigen eine BES12 Client-Version, die die Standortbestimmung unterstützt. Der BES12 Client verwendet den Dienst zur Standortbestimmung auf iOS-Geräten zur Anzeige von deren aktuellem Standort auf einer Karte in BES12.

Hinweis: Der Benutzer muss das Profil für die Standortbestimmung akzeptieren, damit der Standort seines Geräts in der Verwaltungskonsole oder BES12 Self-Service angezeigt werden kann.

Bestimmen des Standorts eines iOS-Geräts

Ein Profil für die Standortbestimmung muss zugewiesen und von Benutzern akzeptiert werden, damit Sie Gerätestandorte auf einer Karte anzeigen können.

1. Klicken Sie in der Menüleiste auf **Benutzer und Geräte**.
2. Klicken Sie auf das Kontrollkästchen für jeden Benutzer eines iOS-Geräts, dessen Standort Sie bestimmen möchten. Sie können bis zu 100 iOS-Geräte zugleich auswählen.
3. Klicken Sie auf .
4. Gehen Sie zum Bestimmen des Standorts eines iOS-Geräts auf der Karte wie folgt vor:

    - Der zuletzt von einem Gerät an BES12 gemeldete Standort ist mit dem Symbol gekennzeichnet. Dieses Symbol zeigt zudem Informationen zu Breiten- und Längengrad des Standorts an sowie zur Zeitdauer, für die der Standort auf dem Gerät aufgezeichnet wurde.

- Der aktuelle Standort des Geräts ist mit dem Symbol gekennzeichnet Dieses Symbol zeigt zudem Informationen zu Breiten- und Längengrad des Standorts an sowie zur Zeitdauer, für die der Standort auf dem Gerät aufgezeichnet wurde.

Simple

Wartung und Überwachung

Überwachen Sie den Status von BES12-Komponenten, und verwenden Sie Protokolle zur Fehlerbehebung.

Verwendung von Protokolldateien

27

Sie können die Protokolldateien verwenden, um Probleme mit den BES12-Komponenten oder -Geräten in Ihrer Unternehmensumgebung zu erkennen und zu lösen. Mit den BES12-Protokollfunktionen können Sie:

- Die Aktivität der BES12-Komponenten mithilfe der Serverprotokolle nachverfolgen
- BES12-Protokolldateidaten an einen SysLog-Server oder an eine Textdatei senden
- Auslesen von Protokolldateien aus BlackBerry 10-Geräten
- App-Aktivitäten auf BlackBerry 10-Geräten überwachen

Verwalten von BES12-Protokolldateien

Die Größe der Protokolldateien variiert abhängig von der Anzahl der Benutzer und Geräte in Ihrer BES12-Umgebung und deren Aktivität. Es empfiehlt sich, die Menge des durch die Protokolldateien eingenommenen Festplattenspeichers zu überwachen und zu steuern. Um zu verhindern, dass sie zu viel Speicherplatz belegen, können Sie eine maximale Dateigröße und eine Debugebene für die Protokolldateien festlegen.

Protokolleinstellungen können Sie auf folgenden Ebenen konfigurieren:

- Globale Protokollierungseinstellungen: Diese Einstellungen gelten für alle BES12-Instanzen in Ihrer Organisation, die auf die gleiche Datenbank zugreifen. Diese Einstellungen umfassen den Speicherort der SysLog-Datei und die maximale Größe für die Protokolldateien.
- Instanzen-Protokollierungseinstellungen: Diese Einstellungen gelten nur für die von Ihnen ausgewählte BES12-Instanz, und Sie heben damit die globalen Einstellungen auf. Diese Einstellungen umfassen die Aktivierung der Option eines lokalen Speicherorts für die Protokolldateien und der Protokollierungsebene für die Protokolldateien.

Konfigurieren der globalen Protokollierungseinstellungen

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Erweitern Sie im linken Fensterbereich die Option **Infrastruktur**. Klicken Sie auf **Anmelden**.
3. Konfigurieren Sie die folgenden globalen Einstellungen entsprechend den Anforderungen Ihrer Organisationsumgebung:

   Hinweis: Bei Änderungen an diesen Einstellungen ist ein Systemneustart erforderlich.

Einstellung	Schritte
Weiterleitung der Systemereignisse an einen SysLog-Server	1. Aktivieren Sie das Kontrollkästchen **SysLog**. Dieses Kontrollkästchen ist standardmäßig deaktiviert. 2. Legen Sie den Hostnamen und den Port für den Syslog-Server fest, an den Sie die BES12-Protokollereignisse weiterleiten möchten.

Einstellung	Schritte
Festlegung der maximalen Dateigröße für die Protokolldateien der BES12-Komponente	Legen Sie im Feld **Maximale Größe für Protokolldateien** die maximale Größe in MB fest, die die einzelnen Protokolldateien erreichen dürfen. Wenn eine Protokolldatei die maximale Größe erreicht, legt BES12 eine neue Version der Protokolldatei an.
Zum Festlegen des maximale Alters für die BES12-Serverprotokolldateien	Geben Sie im Feld **Maximales Alter der Serverprotokolldatei** den maximalen Zeitraum in Tagen ein, für den die Serverprotokolldateien gespeichert werden sollen, bevor sie gelöscht werden. Wenn Sie keinen Wert angeben, werden die Protokolldateien nicht gelöscht.
Festlegung eines Netzwerk-Zielpfads für Protokolldateien der BlackBerry 10-Geräte	Legen Sie im Feld **Netzwerkpfad des Geräteprotokolls** den UNC-Pfad für die Speicherung der Aktivitäts-Protokolldateien fest, die Sie mithilfe der Verwaltungskonsole auslesen.
Maximales Alter der App-Überwachungsprotokolldatei des Geräts	Geben Sie im Feld **Maximales Alter der App-Überwachungsprotokolldatei des Geräts** den maximalen Zeitraum in Tagen ein, für den die App-Überwachungsprotokolldateien gespeichert werden sollen, bevor sie gelöscht werden. Wenn Sie keinen Wert angeben, werden die Protokolldateien nicht gelöscht.

4. Klicken Sie auf **Speichern**.

Konfiguration der Instanzen-Protokollierungseinstellungen

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Erweitern Sie im linken Fensterbereich die Option **Infrastruktur**. Klicken Sie auf **Anmelden**.
3. Erweitern Sie die Serverinstanz, die Sie konfigurieren möchten.
4. Konfigurieren Sie die folgenden Einstellungen entsprechend den Anforderungen Ihrer Organisationsumgebung:

Einstellung	Schritte
Festlegung des Speicherorts, unter dem Protokolldateien der BES12-Komponente gespeichert werden	**Hinweis:** Sie müssen das Kontrollkästchen zum **Aktivieren des lokalen Dateipfads** in den globalen Protokollierungseinstellungen aktivieren, bevor Sie diese Einstellung ändern können. 1. Geben Sie den Pfad ein, unter dem Sie die Server-Protokolldateien speichern möchten. Standardmäßig werden die Protokolldateien unter C:\Program Files\BlackBerry\BES\Logs*yyyymmdd* gespeichert.

Einstellung	Schritte
Festlegen der Detailebene in den Protokolldateien	Wählen Sie in der Dropdown-Liste **Fehlerbehebungsebenen protokollieren** eine der folgenden Optionen aus: • **Info**: Tägliche Aktivitäten, Warnungen und Fehlermeldungen in die Protokolldatei übernehmen. • **Warnen**: Warnungen und Fehlermeldungen in die Protokolldatei übernehmen. Warnungen sind unerwartete Zwischenfälle, für die Sie ggf. in Aktion treten müssen. • **Fehler**: Alle Fehlermeldungen in die Protokolldatei übernehmen. Bei einem Fehlerzustand müssen Sie in der Regel aktiv werden. • **Fehlerbehebung**: Nur Informationen übernehmen, die für die Fehlerbehebung eines Problems erforderlich sind. • **Nachverfolgung**: Zusätzliche Informationen aufzeichnen, die Entwickler bei der weiteren Fehlerbehebung unterstützen. Standardmäßig ist die Fehlerbehebungsebene auf **Info** eingestellt.
Festlegen des Ordners für die App-Überwachungsprotokolle der BlackBerry 10-Geräte	Geben Sie im Feld **Pfad des App-Überwachungsprotokolls des Geräts** den Pfad ein, unter dem Sie die App-Überwachungsprotokolle des Geräts speichern möchten.
Festlegen der maximalen Größe für das App-Überwachungsprotokoll des Geräts	Legen Sie im Feld **Maximale Größe für App-Überwachungsprotokolle** die maximale Größe in MB fest, die die App-Überwachungsprotokolle des Geräts erreichen dürfen. Wenn eine Protokolldatei die maximale Größe erreicht, legt BES12 eine neue Version der Protokolldatei an.

5. Klicken Sie auf **Speichern**.

Ändern des maximalen Alters einer Protokolldatei

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Erweitern Sie im linken Fensterbereich die Option **Infrastruktur**.
3. Klicken Sie auf **Anmelden**.
4. Erweitern Sie **Globale Protokollierungseinstellungen**.
5. Konfigurieren Sie das maximale Alter der Server-Protokolldatei in Tagen.
6. Klicken Sie auf **Speichern**.

Auffinden der Protokolldateien

Standardmäßig wird eine Server-Protokolldatei für jede BES12-Komponente erstellt und täglich auf dem Computer gespeichert, auf dem die Komponente installiert ist. Wenn Sie mehrere BES12-Instanzen installieren, legt jeder Computer seine eigenen Protokolldateien an. BES12 benennt die Protokolldateien *<server_name>_<component_identifier>_<instance>_<yyyymmdd>_<log_number>.<file extension>* (zum Beispiel BBServer01_MDAT_01_20140730_0001.txt).

Die folgenden Protokolldateien stehen in einer BES12-Lösung zur Verfügung:

- Protokolldateien für Komponenten, die für das Verwalten von BlackBerry 10-, iOS-, Android- und Windows Phone-Geräten verwendet werden.

  Protokolldateien sind:

  - ACCS – Tomcat-Zugangsprotokolldateien
  - AFMGR – BlackBerry Affinity Manager-Protokolldateien
  - BGS – BlackBerry Gatekeeping Service-Protokolldateien
  - CORE – BES12 Core-Protokolldateien
  - DISP – BlackBerry Dispatcher-Protokolldateien
  - EVNT – BES12 Core-Ereignis-Protokolldateien
  - MDAT – BlackBerry MDS Connection Service-Protokolldateien
  - TMCT – Tomcat-Serverprotokolldateien
  - UI – BES12-Protokolldateien der Verwaltungskonsole

  Weitere Protokolldateien werden erstellt, wenn Sie erstmalig BES12 installieren.

  Standardmäßig werden diese Protokolldateien unter <Laufwerk>:\Programme\BlackBerry\BES\Logs*<date or folder name>* gespeichert.

- Für BlackBerry Secure Connect Plus werden folgende Protokolldateien verwendet:

  - BSP: BlackBerry Secure Connect Plus-Protokolldateien, in denen Daten zu Verbindungen mit der BlackBerry Secure Connect Plus-App protokolliert werden
  - BSCP-TS: BlackBerry Secure Connect Plus-Core-Protokolldateien, in denen Daten zur BlackBerry Secure Connect Plus-Komponente gespeichert werden

  Die BlackBerry Secure Connect Plus-Protokolldateien werden in <Laufwerk>:\Programme\BlackBerry\BES\Logs \<jjmmtt> gespeichert.

- Für BlackBerry Work Connect Notification Service werden folgende Protokolldateien verwendet:

  - BWCN: BlackBerry Work Connect Notification Service-Protokolldateien

  Die BlackBerry Work Connect Notification Service-Protokolldateien werden in <Laufwerk>:\Programme\BlackBerry \BES\Logs\BWCN*<filename>* gespeichert.

- Protokolldateien für Komponenten, die zur Verwaltung von BlackBerry OS-Geräten (Version 5.0 bis 7.1) (falls verfügbar) verwendet werden

  Standardmäßig werden diese Protokolldateien täglich unter C:\Programme\Research In Motion\BlackBerry Enterprise Server\Logs <*date or folder name*> gespeichert.

  Weitere Informationen finden Sie im Handbuch für Administratoren unter help.blackberry.com/detectlang/bes5.

- BBM-, Telefon-, PIN mit PIN-, SMS/MMS- und Videochat -Protokolle werden im CSV-Format gespeichert und zur Prüfung der App-Aktivitäten verwendet.

  Die App-Überwachungsprotokolle für BlackBerry 10-Geräte werden standardmäßig in *C:\Program Files\BlackBerry\BES\Logs\<yyyymmdd>* gespeichert, während die App-Überwachungsprotokolle für BlackBerry OS-Geräte in *C:\Program Files (x86)\Research in Motion\BlackBerry Enterprise Server\Logs\<yyyymmdd>* gespeichert werden.

Lesen der Protokolldateien

BES12-Protokolldateien werden in zwei Formaten gespeichert: als kommagetrennte Werte und als Textdateien.

BlackBerry Gatekeeping Service-Protokolle, BES12-Paketprotokolle, Protokolle für BlackBerry Messenger Kontakt und Nachricht, Telefonanrufe, PIN, SMS und Videochats werden im CSV-Format gespeichert.

Alle anderen Protokolldateien werden im TXT-Format gespeichert.

Lesen der .csv Protokolldateien

Kommagetrennte Protokolldateien enthalten unterschiedliche Informationen, die davon abhängen, für welche Komponente, für welches Gerät oder für welche Geräte-App sie die Informationen protokollieren. Einige Beispiele für Protokolldateien im Format .csv sind die BlackBerry Gatekeeping Service-Protokolldatei sowie die App-Überwachungsprotokolle des Geräts, wie BBM oder das Telefonanrufprotokoll.

Sie können die in der .csv Protokolldatei enthaltenen Informationen genau bestimmen, da die Informationen in jeder Protokollzeile in einem einfachen und einheitlichen Format aufgeführt sind. Jede Zeile der SMS-Protokolldatei enthält Informationen in folgendem Format:

```
Name.ID,"Email Address","Type of Message","To","From","Callback Phone
Number","Body","Send/Received Date","Server Log Date","Overall Message
Status","Command","UID"
```

Jede Zeile einer Telefonprotokolldatei zeigt Informationen in folgendem Format:

```
Name.ID,"Type of Call","Name","Phone Number","Start Date","Server Log Date","Elapsed
Time","Memo","Command","UID","Phone Line"
```

Lesen von .txt Protokolldateien

Protokolldateien, die als .txt-Dateien gespeichert werden, haben zwei Basisformate:

- Das erste Format, das mit einer numerischen Ebenenanzeige beginnt, stellt die Informationen auf folgende Weise bereit:

  ```
  Level Date Thread Duration CID Message
  ```

  Beispiel:

  ```
  <#03>[30000] (09/10 00:00:00.122):{0x520} [DIAG] EVENT=Thread_report,
  THREADID=0x1390, THREADNAME="SRPReceiverHandler"
  ```

- Das zweite Format, das in der Regel mit Datum und Zeit beginnt, stellt die Informationen auf folgende Weise bereit:

  ```
  TimeStamp Hostname AppName ProcessId MessageID [StructuredData] Message
  ```

  Beispiel:

  ```
  2014-09-10 00:00:02.431-0400 - CORE {scheduler-thread-6}
  logging.feature.device.metadata.scheduler|logging.component.default.service
  [{{Correlation-Id,703c11c7-acc3-4a09-9564-d94f265ffd59}}] - INFO CORE Version:
  5.4.0, Product Version: 3.4.0
  ```

Je nach der zu protokollierenden Komponente bzw. Funktion gibt es einige Unterschiede. Alle als `.txt`-Dateien gespeicherten Protokolldateien enthalten jedoch die folgenden Basisinformationen.

Objekt	Beschreibung
Datum oder Zeitstempel	Ein Zeitstempel in der Form <Datum>T<Zeit><Abweichung zur UTC-Zeit>. Datum/Zeit gibt das Datum und die Uhrzeit eines bestimmten Ereignisses an. **Hinweis:** Datum und Zeitstempel werden in der Zeit des lokalen Servers angegeben.
Ebene	Die Ereignisebene gibt die Art des Protokolleintrags an. Im Allgemeinen lassen sich die Ereignisse in die folgenden Kategorien einteilen: • ERR = Fehler • WARN = Warnung • INFO = Information ENV = Umgebung • DEBUG = Fehlerbehebung • Sonstiges ◦ DIAG = Diagnose ◦ TRAC = Verfolgung

Objekt	Beschreibung
	Bei einigen Protokolldateien wird die Ebene mit einem numerischen Wert in folgendem Format angegeben: • [10000] = Fehler • [20000] = Warnung • [30000] = Informativ • [40000] = Informationen zur Fehlerbehebung • [50000] = Andere
Kennzeichnung der Komponente oder Hostname	Anhand der Kennzeichnung der Komponente oder des Hostnamens können Sie erkennen, auf welche Komponente sich diese Protokolldatei bezieht. Während es in einigen Fällen eindeutig ist (zum Beispiel, wenn CORE oder MDS-CS angegeben wird), ist es in anderen Fällen weniger eindeutig, sodass ein numerisches Kennzeichen verwendet wird.
Thread-ID	Der Thread gibt an, welcher Prozess ein Ereignis durchgeführt hat.
Dauer	Die Dauer gibt an, wie lange das Ereignis gedauert hat (in der Regel Sekunden).
Nachricht	Die Nachricht gibt die Aktivität an und beschreibt die Art des Ereignisses. Eine Nachricht könnte Informationen über die Hardware, die ausgeführte Software oder über das aufgetretene Problem enthalten.

Protokolldateiebenen

Ebene	Beschreibung
DEBUG	Diese Ebene legt die Informationen fest, die zur Fehlerbeseitigung bei Codierungsproblemen nützlich sind. Die Ereignisse können Folgendes enthalten: • Status der Ressourcen, die vermutlich einen Fehler aufweisen • Übergänge zwischen internen und externen Komponenten • REST-Anforderungen an BES12 Core • Anforderungen an Microsoft Active Directory
ERROR	Diese Ebene spezifiziert einen Fehlerzustand, der Maßnahmen von Ihnen oder von einem Support-Experten erfordert. Die Ereignisse können Folgendes enthalten: • Verschlüsselungsausnahmen

Ebene	Beschreibung
	• Ausnahmen auf der Datenebene • Wiederherstellbare Verschlüsselungsausnahmen
INFO	Diese Ebene legt die normalen Systemereignisse fest, die Administratoren oder Support-Experten ggf. einsehen möchten. Diese Ebene ist die Standardprotokollebene für BES12.
TRACE	Diese Ebene legt Informationen fest, die für Personen mit Entwickler-Kenntnissen nützlich sind. Hierzu gehören auch Informationen, die für Klassen und Methoden-Nachverfolgung, Methodenparameter etc. verwendet werden.
WARN	Diese Ebene kann auf einen Warnzustand oder auf erforderliche Maßnahmen hinweisen, oder anzeigen, dass ein unerwartetes Ereignis aufgetreten ist. Die Ereignisse können Folgendes enthalten: • Inkonsistente Daten • Unerwartete Anforderungen • Autorisierungsfehler • Authentifizierungsfehler

Protokolldateien zur Fehlerbehebung verwenden

Komponenten-bezeichner	Protokollierungskomponente	Beschreibung
ACCS	Apache Tomcat-Serverzugriff-Protokolldateien	In den Apache Tomcat-ACCS-Protokolldateien werden alle Zugriffsanforderungen für die BES12-Webdienste aufgezeichnet. Sie können diese Protokolldateien verwenden, wenn Sie überprüfen möchten, ob Zugriffsanforderungen für die BES12-Webdienste erfolgreich oder nicht erfolgreich waren.
AFMGR	BlackBerry Affinity Manager	BlackBerry Affinity Manager umfasst Daten zur Funktionalität und zum Verfügbarkeitsstatus, wenn Sie mehr als einen BlackBerry Affinity Manager in der Umgebung des Unternehmens haben. Außerdem können Sie Fehler in folgenden Zusammenhängen beheben: • Konnektivität zwischen BES12 und der BlackBerry Infrastructure

Komponenten-bezeichner	Protokollierungskomponente	Beschreibung
		• Konnektivität zwischen BES12 und BlackBerry 10-Geräten • Integritätsprobleme, die zu einer Änderung von BlackBerry Affinity Manager führen.
BGS	BlackBerry Gatekeeping Service	Diese Protokolldateien können Sie verwenden, um Fehler in folgenden Zusammenhängen zu beheben: • Geräte, die nicht in einer Umgebung aktiviert werden können, in der BlackBerry Gatekeeping Service verwendet wird. • Konnektivität zu Ihrem BlackBerry Gatekeeping Service • Konnektivität zwischen BES12 und der BlackBerry Infrastructure • BlackBerry 10-Aktivierungen und Senden von Richtlinien und Profilen • iOS, Android und Windows Phone-Konnektivität

BSCP	BlackBerry Secure Connect Plus	Protokolliert Daten über die BlackBerry Secure Connect Plus-Komponente.
		Sie können anhand dieser Protokolldateien prüfen, ob BlackBerry Secure Connect Plus mit der BlackBerry Infrastructure verbunden ist. Beispiel:
		`2015-01-19T13:17:47.540-0500 - BSCP {TcpClientConnectorNio#2} logging.feature.bscp.service| logging.component.bscp.pss.bcp [{}] - DEBUG Received Ping from [id: 0x60bce5a3, / 10.90.84.22:28231 => stratos.bcp.bblabs.rim.net/ 206.53.155.152:3101], responding with Pong.`
		`2015-01-19T13:18:22.989-0500 - BSCP {ChannelPinger#1} logging.feature.bscp.service| logging.component.bscp.pss.bcp [{}] - DEBUG Sending Ping to [id: 0xb4a1677a, / 10.90.84.22:28232 => stratos.bcp.bblabs.rim.net/ 206.53.155.152:3101]`

CORE	BES12 Core	Diese Protokolldateien können Sie verwenden, um Fehler in folgenden Zusammenhängen zu beheben: • Core-Dienste oder -Transaktionen • Datenmigration von BES10

Komponenten-bezeichner	Protokollierungskomponente	Beschreibung
DISP	BlackBerry Dispatcher	Diese Protokolldateien können Sie verwenden, um Fehler in folgenden Zusammenhängen zu beheben: • Konnektivität zwischen BES12 und der BlackBerry Infrastructure • Konnektivität zwischen BES12 und BlackBerry 10-Geräten
EVNT	BES12 Core	Sie können diese Protokolldateien verwenden, um Benachrichtigungen zu bestimmten Ereignissen im BES12 Core zu suchen.
MDAT	BlackBerry MDS Connection Service	Diese Protokolldateien können Sie verwenden, um Fehler in folgenden Zusammenhängen zu beheben: • BlackBerry 10-Geräteapps • App-Push-Fehler • App-Push-Authentifizierungsfehler

BSCP-TS	BlackBerry Secure Connect Plus Core	Protokolliert Daten für Verbindungen mit dem BlackBerry Secure Connect Plus-Client.
		Sie können anhand dieser Protokolldateien überprüfen, ob BlackBerry Secure Connect Plus Aufrufe vom BlackBerry Secure Connect Plus-Client auf Geräten empfangen kann. Beispiel:
		`47: [14:13:21.231312][][3][AsioTurnSocket-1] Connected, host=68-171-243-141.rdns.blackberry.net`
		`48: [14:13:21.239312][][3][AsioTurnSocket-1] Creating TURN allocation`
		`49: [14:13:21.405121][][3][AsioTurnSocket-1] TURN allocation created`
		Zum Überprüfen, ob Geräte den sicheren Tunnel verwenden. Beispiel:
		`74: [10:39:45.746926][][3][Tunnel-2FFEC51E] Sent: 2130.6 KB (1733), Received: 201.9 KB (1370), Running: 00:07:00.139249`

ROUT	BlackBerry Router	Diese Protokolldateien können Sie verwenden, um Fehler in folgenden Zusammenhängen zu beheben: • BlackBerry Router-Installation • Konnektivität zwischen BES12 und der BlackBerry Router

Komponenten-bezeichner	Protokollierungskomponente	Beschreibung
		• Konnektivität zwischen BES12 und der BlackBerry Infrastructure • Konnektivität zwischen dem BlackBerry Router und der BlackBerry Infrastructure • Konnektivität zwischen Geräten und BES12 **Hinweis:** Die BlackBerry Router-Protokolldateien sind nur dann verfügbar, wenn Sie den BlackBerry Router in Ihrer Unternehmensumgebung installiert haben.
TMCT	Apache Tomcat-Server-Protokolldateien	Die Apache Tomcat TMCT-Protokolldateien zeichnen alle Aktivitäten der Apache Tomcat-Webdienste auf. Sie können diese Protokolldateien verwenden, wenn Sie Fehler im Zusammenhang mit der Verwaltungskonsole beheben.
UI	Verwaltungskonsole	Sie können diese Protokolldateien verwenden, wenn Sie Fehler im Zusammenhang mit der Verwaltungskonsole beheben.
Diese Protokolldateien haben keinen Komponentenbezeichner als Präfix	BlackBerry Work Connect Notification Service	Sie können diese Protokolldateien verwenden, um Fehler im Zusammenhang mit iOS-Geräten zu beheben, die keine Benachrichtigungen zu neuen oder geänderten Elementen empfangen.

Überwachen der App-Aktivität auf BlackBerry 10- und BlackBerry OS-Geräten

Sie können die Geräteprotokolle zur Überwachung der App-Aktivität bei BlackBerry 10-Geräten mit den Aktivierungsarten„ Nur geschäftlicher Bereich “und „Geschäftlich und persönlich – Reguliert“ und bei BlackBerry OS-Geräten (Version 5.0 bis 7.1) verwenden.

Zur Erstellung dieser Protokolldateien müssen Sie die folgende IT-Richtlinienregel konfigurieren:

IT-Richtlinienregel für BlackBerry 10	IT-Richtlinienregel für BlackBerry OS-Geräte	
BBM-Protokolle synchronisieren	Drahtlose BlackBerry Messenger-Synchronisierung deaktivieren	Diese Regel legt fest, ob ein Gerät die Protokolle aus BlackBerry Messenger mit BES12 synchronisiert.
Telefonprotokolle synchronisieren	Drahtlose Synchronisierung von Telefonanrufprotokollen deaktivieren	Diese Regel legt fest, ob ein Gerät das Anrufprotokoll für die Telefon-App mit BES12 synchronisiert.
PIN mit PIN-Protokollen synchronisieren	Drahtlose Synchronisierung von PIN-Nachrichten deaktivieren	Diese Regel legt fest, ob ein Gerät die Protokolle für PIN-Nachrichten mit BES12 synchronisiert.
SMS/MMS-Protokolle synchronisieren	Drahtlose Synchronisierung von SMS-Nachrichten deaktivieren	Diese Regel legt fest, ob ein Gerät die Protokolle für SMS-Textnachrichten und MMS-Nachrichten mit BES12 synchronisiert.
Videochat-Protokolle synchronisieren	Gilt nicht für BlackBerry OS-Geräte	Diese Regel legt fest, ob ein BlackBerry 10-Gerät die Protokolle für die BBM Video-Funktion mit BES12 synchronisiert.

Die App-Überwachungsprotokolle für BlackBerry 10-Geräte werden standardmäßig in *C:\Program Files\BlackBerry\BES\Logs\<yyyymmdd>* gespeichert, während die App-Überwachungsprotokolle für BlackBerry OS-Geräte in *C:\Program Files (x86)\Research in Motion\BlackBerry Enterprise Server\Logs\<yyyymmdd>* gespeichert werden.

Anzeigen der Geräteaktionen

Aktionen, die auf einem Gerät aufgrund von Befehlen durchgeführt wurden oder werden, die Sie mit der BES12-Verwaltungskonsole gesendet haben, wie zum Beispiel Sperren eines Gerätes, Deaktivieren des geschäftlichen Bereichs oder Löschen von Gerätedaten.

Die Verfügbarkeit dieser Befehle hängt vom Gerät und von der Aktivierungsart ab.

Ein Gerätebefehl kann den folgenden Status haben:

- Befehl abgebrochen
- Befehl vom Gerät ausgeführt
- Befehl an das Gerät übertragen
- Befehlübertragung vom Gerät bestätigt
- Befehl fehlgeschlagen
- Befehl wird verarbeitet
- Benachrichtigung vom Gerät bestätigt

- Benachrichtigung an das Gerät gesendet
- In Warteschlange

Anzeigen der Geräteaktionen

1. Suchen Sie auf der Seite **Benutzer und Geräte** das Benutzerkonto, und klicken Sie es an.
2. Klicken Sie auf die Registerkarte des Gerätes, für das Sie die Geräteaktionen aufrufen möchten.
3. Klicken Sie auf **Anzeigen der Geräteaktionen**.

Auslesen von Protokolldateien aus Geräten

Mithilfe der folgenden Methoden können Sie Protokolldateien aus BlackBerry 10-, Android- und Windows Phone-Geräten auslesen:

Methode	Beschreibung
Auslesen von Protokolldateien aus BlackBerry 10-Geräten	Sie können Protokolldateien aus BlackBerry 10-Geräten auslesen, um die Fehlerbehebung zu erleichtern. Ein Speicherauszug der Protokolldateien zu dem Gerät wird jedes Mal erfasst, wenn Sie den Gerätebefehl zum Auslesen der Dateien verwenden. Die Benutzer werden darüber informiert, dass Sie während der Geräteaktivierung Systemprotokolldateien erfassen können, und erhalten je nach den Geräteeinstellungen ggf. eine erneute Benachrichtigung, wenn Sie den Befehl zum Auslesen der Protokolldateien absenden.
Versenden von BlackBerry 10-Geräteprotokolldateien an BlackBerry Technical Support Services	Sie können BlackBerry 10-Geräteprotokolle an BlackBerry Technical Support Services versenden, indem Sie die IT-Richtlinienregel „Protokolle an BlackBerry senden“ verwenden, die festlegt, ob das Gerät Protokolldateien erzeugen und senden kann.
Versenden von Protokolldateien vom BES12 Client	Benutzer von Android- oder Windows Phone-Geräten können die Geräteprotokolldateien per E-Mail an ihren Administrator senden, indem Sie das Menü **Hilfe** in BES12 Client verwenden.

Auslesen von Protokolldateien aus BlackBerry 10-Geräten

Um Protokolldateien von BlackBerry 10-Geräten auszulesen, müssen Sie die folgenden Voraussetzungen erfüllen:

- Auf dem BlackBerry 10-Gerät muss BlackBerry 10 OS Version 10.3.1 oder höher ausgeführt werden.
- Bei einem BlackBerry 10-Gerät, das mit der Aktivierungsart „Geschäftlich und persönlich – Unternehmen“ aktiviert wurde, muss der Gerätebenutzer die Remote Log Collection aktivieren, damit der Administrator die Protokolldateien auslesen kann. Wenn die Remote Log Collection nicht aktiviert ist, kann die Schaltfläche zum Abrufen der Geräteprotokolle in der BES12-Verwaltungskonsole nicht ausgewählt werden.

Bei den Geräten, die mit den Aktivierungsarten „Geschäftlich und persönlich – Reguliert“ oder „Nur geschäftlicher Bereich“ aktiviert wurden, ist die Remote Log Collection standardmäßig aktiviert.

Standardmäßig kann die Rolle „Junior HelpDesk“ keine Protokolldateien auslesen.

1. Wählen Sie auf der Registerkarte **Benutzer und Geräte** den Benutzer aus, für den Sie die Protokolldateien auslesen möchten.
2. Wählen Sie das Gerät aus, für das Sie die Protokolldateien auslesen möchten.
3. Klicken Sie auf **Geräteprotokolle abrufen**.

Wenn Sie fertig sind:

Rufen Sie die Geräteprotokolldateien ab. Standardmäßig werden die Protokolldateien unter C:\Program Files\BlackBerry\BES\Logs\device_logs gespeichert.

BlackBerry 10-Geräteprotokolldateien an BlackBerry Technical Support Services senden

Sie können ein BlackBerry 10-Gerät so konfigurieren, dass es Protokolldateien an BlackBerry Technical Support Services senden kann. Sie können die IT-Richtlinienregel **Protokolle an BlackBerry senden** verwenden, die festlegt, ob das Gerät Protokolldateien erzeugen und senden kann.

Der Benutzer muss ein offenes Ticket bei BlackBerry Technical Support Services haben und beim Einreichen der Geräteprotokolldateien die Ticketnummer angeben. Wenn der Benutzer keine gültige Support-Ticketnummer oder nicht die zum Support-Ticket passende E-Mail-Adresse oder PIN-Nummer angibt, zeigt das Gerät beim Versuch, die Geräteprotokolldateien zu versenden, einen Fehler an.

Versenden von Protokolldateien vom BES12 Client

1. Tippen Sie auf dem Gerät auf das Symbol BES12.
2. Tippen Sie auf **Hilfe**.
3. Tippen Sie auf **Weitere**.
4. Tippen Sie auf **Bug Report**.
5. Wählen Sie zum Versenden der Protokolldatei das E-Mail-Konto auf dem Gerät aus.
6. Tippen Sie auf **Senden**.
    - Android-Protokolldateien werden als ZIP-Datei an die E-Mail angehängt
    - Windows Phone-Geräteprotokolldateien werden im Nachrichtentext der E-Mail angezeigt

Überwachungsaktionen in BES12

28

BES12 führt eine Protokolldatei der Aktionen, die Sie zur Untersuchung von Problemen verwenden können. BES12 zeichnet beispielsweise Aktionen auf, die in den Menüs „Benutzer und Geräte“, „Richtlinien und Profile“, „Gruppen“ und „Apps“ ausgeführt wurden, sowie Änderungen an den Einstellungen im Menü „Einstellungen“. Die Details der Aktionen werden auf der Benutzeroberfläche angezeigt und können zu Überwachungszwecken verwendet werden. Sie können die Liste der Aktionen filtern, um nur die Aktionen anzuzeigen, die für Ihre Untersuchung relevant sind.

Zu weiteren Analyse- oder Reporting-Zwecken können Sie das gefilterte Protokoll in eine .csv-Datei exportieren.

Konfigurieren von Überwachungseinstellungen

Sie können die Überwachung in BES12 aktivieren oder deaktivieren. Wenn die Überwachung aktiviert ist, können Sie die Speicherdauer für Datensätze, die Anzahl der anzuzeigenden Ergebnisse und den Zeitpunkt für das Löschen alter Datensätze auswählen. Wenn die Überwachung deaktiviert ist, werden alle Datensätze gelöscht.

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Erweitern Sie im linken Fensterbereich die Option **Infrastruktur**.
3. Klicken Sie auf die **Überwachungskonfiguration**.
4. Klicken Sie im rechten Fensterbereich auf .
5. Führen Sie im Feld **Überwachung** eine der folgenden Aktionen aus:

Aufgabe	Schritte
Aktivieren der Überwachung	1. Klicken Sie auf **Aktiviert**. 2. Geben Sie im Feld für das **Aufbewahrung der Überwachungsaufzeichnungen** die Anzahl der Tage ein, für die der Datensatz gespeichert werden soll. 3. Geben Sie im Feld für die **Maximale Anzahl an Einträgen** die maximale Anzahl der Datensätze ein, die auf der Benutzeroberfläche angezeigt werden soll. Wenn die Anzahl der Datensätze diesen Wert überschreitet, muss der Administrator den Datumsbereich verkürzen oder eine Kategorie auswählen, um die Anzahl der Datensätze zu verringern. 4. Wählen Sie im Feld für die **Tägliche Löschzeit (UTC-Zeitzone)** die Tageszeit aus, zu der alte Datensätze gelöscht werden sollen.
Deaktivieren der Überwachung und Entfernen aller Datensätze	1. Klicken Sie auf **Deaktiviert**.

6. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind:

- Führen Sie einen Neustart des BES12 Core-Dienstes auf jedem Computer aus, der eine BES12-Instanz hostet.
- Melden Sie sich erneut bei der Verwaltungskonsole an.

Anzeigen und Filtern des Überwachungsprotokolls

1. Klicken Sie in der Menüleiste auf **Audit**.
2. Klicken Sie im linken Fensterbereich auf **Bearbeiten**.
3. Wählen Sie eine Kategorie und einen Datumsbereich aus. Klicken Sie auf **Senden**.
4. Klicken Sie unter **Filter** auf eine Kategorie, um diese zu erweitern.
5. Wählen Sie die Filter aus, die Sie anwenden möchten, und klicken Sie auf **Senden**.
6. Optional klicken Sie im rechten Fensterbereich auf das + in einer Spaltenüberschrift. Wählen Sie die Spalten aus, die Sie anzeigen möchten.
7. Falls notwendig, führen Sie einen der folgenden Schritte aus:
    - Zum Entfernen eines Filters klicken Sie auf ✕ neben dem Filter, den Sie entfernen möchten.
    - Zum Entfernen aller Filter klicken Sie auf **Alle entfernen**.

Wenn Sie fertig sind: Exportieren Sie das Überwachungsprotokoll ggf. in eine .csv-Datei.

Exportieren des Überwachungsprotokolls in eine .csv-Datei

Wenn Sie das Überwachungsprotokoll in eine .csv-Datei exportieren, enthält diese Datei die von Ihnen gefilterten Daten.

1. Klicken Sie in der Menüleiste auf **Audit**.
2. Filtern Sie im linken Fensterbereich ggf. das Überwachungsprotokoll, um nur die Daten anzuzeigen, die Sie in die .csv-Datei aufnehmen möchten.
3. Klicken Sie auf ➔, und speichern Sie die Datei.

Löschen alter Überwachungsdatensätze

Sie können alte Überwachungsdatensätze vor dem nächsten täglichen Löschzeitpunkt löschen.

1. Klicken Sie in der Menüleiste auf **Einstellungen**.

2. Erweitern Sie im linken Fensterbereich die Option **Infrastruktur**.
3. Klicken Sie auf die **Überwachungskonfiguration**.
4. Klicken Sie auf **Jetzt löschen**.
5. Klicken Sie auf **Löschen**.

Verwenden von SNMP zur Überwachung von BES12

29

Mithilfe von SNMP-Tools von Drittherstellern können Sie die Aktivität von BES12 überwachen.

Weitere Informationen zur Konfiguration von SNMP zur Überwachung von BES12 Core, BlackBerry Secure Connect Plusund andere BES12-Komponenten finden Sie in der Dokumentation zur Konfiguration.

SNMP-Zähler für Enterprise-Konnektivität

Die folgenden Tabellen enthalten Informationen über einige wichtige SNMP-Zähler zur Überwachung der Leistung und Aktivität von BES12-Komponenten:

BlackBerry Router

Gruppe	Tabelle	Zähler
routerProcess .1.3.6.1.4.1.3530.8.7.35.5	routerProcInfoTable .1.3.6.1.4.1.3530.8.7.35.5.2 Überwachung auf PID-Änderungen	routerProcInfoTablePID .1.3.6.1.4.1.3530.8.7.35.5.2.1.1 Ganze Zahl Numerischer Bezeichner für den Prozess
routerStatistics .1.3.6.1.4.1.3530.8.7.35.20	routerBaseStatsTable .1.3.6.1.4.1.3530.8.7.35.20.5	routerBaseStatsTableSocksConnections .1.3.6.1.4.1.3530.8.7.35.20.5.1.6 Zahl der aktuell vom BlackBerry Router bereitgestellten SOCKS-Verbindungen
routerEvents .1.3.6.1.4.1.3530.8.7.35.30	routerEventsServiceStartEvent .1.3.6.1.4.1.3530.8.7.35.30.2 Trap Legt fest, dass der Dienst für die Komponente gestartet wurde.	
	routerEventsServiceStopEvent .1.3.6.1.4.1.3530.8.7.35.30.3 Trap	

Gruppe	Tabelle	Zähler
	Legt fest, dass der Dienst für die Komponente angehalten wurde.	
routerSOCKSTrafficStats .1.3.6.1.4.1.3530.8.7.35.45	routerRouterSOCKSTrafficStatsTable .1.3.6.1.4.1.3530.8.7.35.45.5	routerRouterSOCKSTrafficStatsTableBytesReceived .1.3.6.1.4.1.3530.8.7.35.45.5.1.4 Counter64 Gesamtzahl der über SOCKS-Verbindungen empfangenen Bytes
		routerRouterSOCKSTrafficStatsTableBytesSent .1.3.6.1.4.1.3530.8.7.35.45.5.1.6 Counter64 Gesamtzahl der über SOCKS-Verbindungen gesendeten Bytes
		routerRouterSOCKSTrafficStatsTableReceiveTransactions .1.3.6.1.4.1.3530.8.7.35.45.5.1.8 Counter64 Gesamtzahl der über SOCKS-Verbindungen erfolgten Empfangsvorgänge
		routerRouterSOCKSTrafficStatsTableSendTransactions .1.3.6.1.4.1.3530.8.7.35.45.5.1.10 Counter64 Gesamtzahl der über SOCKS-Verbindungen erfolgten Sendevorgänge
routerSOCKSConn .1.3.6.1.4.1.3530.8.7.35.130	routerSOCKSConnSOCKSConnConfigTable .1.3.6.1.4.1.3530.8.7.35.130.10	routerSOCKSConnSOCKSConnConfigTableDownstreamSocksHost .1.3.6.1.4.1.3530.8.7.35.130.10.1.2 Oktettzeichenfolge

Gruppe	Tabelle	Zähler
		Hostname des nachfolgenden Endpunkts
		routerSOCKSConnSOCKSConnConfigTableUpstreamSocksHost .1.3.6.1.4.1.3530.8.7.35.130.10.1.4 Oktettzeichenfolge Hostname des voranstehenden Endpunkts
		routerSOCKSConnSOCKSConnConfigTableUpstreamSocksPort .1.3.6.1.4.1.3530.8.7.35.130.10.1.6 Ganze Zahl Port des voranstehenden Endpunkts
	routerSOCKSConnSOCKSConnStateTable .1.3.6.1.4.1.3530.8.7.35.130.15	routerSOCKSConnSOCKSConnStateTableConnected .1.3.6.1.4.1.3530.8.7.35.130.15.1.2 Ganze Zahl Gibt an, ob die Verbindung hergestellt wurde.
		routerSOCKSConnSOCKSConnStateTableLastConDate .1.3.6.1.4.1.3530.8.7.35.130.15.1.4 Ganze Zahl Zeitpunkt, zu dem die Verbindung das letzte Mal erfolgreich hergestellt wurde
	routerSOCKSConnSOCKSConnEvents .1.3.6.1.4.1.3530.8.7.35.130.140	routerSOCKSConnSOCKSConnEventsConnectEvent .1.3.6.1.4.1.3530.8.7.35.130.140.2 Trap Gibt an, dass die Verbindung hergestellt wurde.

Gruppe	Tabelle	Zähler
		routerSOCKSConnSOCKSConnEventsDisconnectEvent .1.3.6.1.4.1.3530.8.7.35.130.140.3 Trap Gibt an, dass die Verbindung verloren wurde.

BlackBerry Affinity Manager

Gruppe	Tabelle	Zähler
affinitymgrProcess .1.3.6.1.4.1.3530.8.7.145.5	affinitymgrProcInfoTable .1.3.6.1.4.1.3530.8.7.145.5.2	Überwachung auf PID-Änderungen in: affinitymgrProcInfoTablePID .1.3.6.1.4.1.3530.8.7.145.5.2.1.1 Ganze Zahl Numerischer Bezeichner für den Prozess
affinitymgrConfig .1.3.6.1.4.1.3530.8.7.145.10	affinitymgrFailoverAssignmentConfigTable .1.3.6.1.4.1.3530.8.7.145.10.25 Überwachung auf Lastverteilungskonfiguration	affinitymgrFailoverAssignmentConfigTableMinimumDifference .1.3.6.1.4.1.3530.8.7.145.10.25.1.4 Ganze Zahl Mindestdifferenz bei Benutzergeräten zwischen BES12-Instanzen, bei welcher der Lastausgleicher eingreift.
		affinitymgrFailoverAssignmentConfigTableMaximumBatchSize .1.3.6.1.4.1.3530.8.7.145.10.25.1.6 Ganze Zahl Maximalzahl der Benutzergeräte pro Einzelzuweisung
		affinitymgrFailoverAssignmentConfigTableMaximumPerServer .1.3.6.1.4.1.3530.8.7.145.10.25.1.8 Ganze Zahl

Gruppe	Tabelle	Zähler
		Maximalzahl der Benutzergeräte, die einer BES12-Instanz zugewiesen werden können
	affinitymgrRcpConfigTable .1.3.6.1.4.1.3530.8.7.145.10.30	affinitymgrRcpConfigTableNumProcThreads .1.3.6.1.4.1.3530.8.7.145.10.30.1.2 Ganze Zahl Zahl der Threads, die RCP-Verbindungen verarbeiten
affinitymgrRCPTrafficStats .1.3.6.1.4.1.3530.8.7.145.15	affinitymgrRCPStatsTable .1.3.6.1.4.1.3530.8.7.145.15.5	affinitymgrRCPStatsTableBytesReceived .1.3.6.1.4.1.3530.8.7.145.15.5.1.4 Counter64 Gesamtzahl der über RCP-Verbindungen empfangenen Bytes
		affinitymgrRCPStatsTableBytesSent .1.3.6.1.4.1.3530.8.7.145.15.5.1.6 Counter64 Gesamtzahl der über RCP-Verbindungen gesendeten Bytes
		affinitymgrRCPStatsTableReceiveTransactions .1.3.6.1.4.1.3530.8.7.145.15.5.1.8 Counter64 Gesamtzahl der über RCP-Verbindungen erfolgten Empfangsvorgänge
		affinitymgrRCPStatsTableSendTransactions .1.3.6.1.4.1.3530.8.7.145.15.5.1.10 Counter64 Gesamtzahl der über RCP-Verbindungen erfolgten Sendevorgänge

Gruppe	Tabelle	Zähler
		affinitymgrRCPStatsTableExternalRcpConnections .1.3.6.1.4.1.3530.8.7.145.15.5.1.12 Ganze Zahl Gesamtzahl der externen RCP-Verbindungen
		affinitymgrRCPStatsTableInternalSrvConnections .1.3.6.1.4.1.3530.8.7.145.15.5.1.14 Ganze Zahl Gesamtzahl der internen Serververbindungen
affinitymgrHA .1.3.6.1.4.1.3530.8.7.145.20	affinitymgrHAStatsTable .1.3.6.1.4.1.3530.8.7.145.20.20	affinitymgrHAStatsTableHAMode .1.3.6.1.4.1.3530.8.7.145.20.20.1.2 Ganze Zahl Gibt an, ob der Hochverfügbarkeitsmodus der Komponente „primär“ oder „standby“ ist 1 = primär
affinitymgrEvents .1.3.6.1.4.1.3530.8.7.145.30	affinitymgrEventsServiceStartEvent .1.3.6.1.4.1.3530.8.7.145.30.2 Trap	
	affinitymgrEventsServiceStopEvent .1.3.6.1.4.1.3530.8.7.145.30.3 Trap	
affinitymgrDatabaseConn .1.3.6.1.4.1.3530.8.7.145.90	affinitymgrDatabaseConnBaseConfigTable .1.3.6.1.4.1.3530.8.7.145.90.5	affinitymgrDatabaseConnBaseConfigTableLastModTime .1.3.6.1.4.1.3530.8.7.145.90.5.1.1 Ganze Zahl Zeitpunkt der letzten Änderung eines Wertesatzes

Gruppe	Tabelle	Zähler
		affinitymgrDatabaseConnBaseConfigTableEndB .1.3.6.1.4.1.3530.8.7.145.90.5.1.6 Oktettzeichenfolge Namen der Verbindungsendpunkte
	affinitymgrDatabaseConnConnectionStatsTable .1.3.6.1.4.1.3530.8.7.145.90.15	affinitymgrDatabaseConnConnectionStatsTableConnected .1.3.6.1.4.1.3530.8.7.145.90.15.1.2 Ganze Zahl Gibt an, ob die Verbindung hergestellt wurde.
		affinitymgrDatabaseConnConnectionStatsTableLastConDate .1.3.6.1.4.1.3530.8.7.145.90.15.1.4 Ganze Zahl Zeitpunkt, zu dem die Verbindung mit der BES12-Datenbank das letzte Mal erfolgreich hergestellt wurde
		affinitymgrDatabaseConnConnectionStatsTableLastErrRsn .1.3.6.1.4.1.3530.8.7.145.90.15.1.6 Oktettzeichenfolge Grund des letzten Verbindungsfehlers
		affinitymgrDatabaseConnConnectionStatsTableLastErrCode .1.3.6.1.4.1.3530.8.7.145.90.15.1.8 Ganze Zahl Fehlercode des zuletzt bei der BES12-Datenbankverbindung aufgetretenen Fehlers. Weitere Informationen enthalten die Protokolldateien.

Gruppe	Tabelle	Zähler
		affinitymgrDatabaseConnConnectionStatsTableLastErrorTime .1.3.6.1.4.1.3530.8.7.145.90.15.1.10 Ganze Zahl Zeitpunkt des letzten Fehlschlagens der Verbindung
		affinitymgrDatabaseConnConnectionStatsTableNumTrans .1.3.6.1.4.1.3530.8.7.145.90.15.1.12 Ganze Zahl Zahl der an die BES12-Datenbank gesendeten SQL-Transaktionen
		affinitymgrDatabaseConnConnectionStatsTableAvgRspTime .1.3.6.1.4.1.3530.8.7.145.90.15.1.14 Ganze Zahl Durchschnittliche Antwortzeit der Verbindung
		affinitymgrDatabaseConnConnectionStatsTableErrs .1.3.6.1.4.1.3530.8.7.145.90.15.1.16 Ganze Zahl Zahl der bei der Datenbankverbindung aufgetretenen Fehler
	affinitymgrDatabaseConnEvents .1.3.6.1.4.1.3530.8.7.145.90.20	
	affinitymgrDatabaseConnEventsConnectEvent .1.3.6.1.4.1.3530.8.7.145.90.20.2 Trap	

Gruppe	Tabelle	Zähler
	affinitymgrDatabaseConnEventsDisconnectEvent .1.3.6.1.4.1.3530.8.7.145.90.20.3 Trap	
affinitymgrExternalRcpConn .1.3.6.1.4.1.3530.8.7.145.100	affinitymgrExternalRcpConnRCPConnStatsTable .1.3.6.1.4.1.3530.8.7.145.100.15	affinitymgrExternalRcpConnRCPConnStatsTableConnected .1.3.6.1.4.1.3530.8.7.145.100.15.1.2 Ganze Zahl Gibt an, ob die Verbindung mit der BES12-Datenbank hergestellt wurde.
		affinitymgrExternalRcpConnRCPConnStatsTableLastConDate .1.3.6.1.4.1.3530.8.7.145.100.15.1.4 Ganze Zahl Zeitpunkt, zu dem die Verbindung das letzte Mal erfolgreich hergestellt wurde
		affinitymgrExternalRcpConnRCPConnStatsTableLastErrCode .1.3.6.1.4.1.3530.8.7.145.100.15.1.6 Ganze Zahl Fehlercode des letzten Verbindungsfehlers. Weitere Informationen enthalten die Protokolldateien. Wenn die Verbindung mit der BlackBerry Infrastructure fehlschlägt, ist der Wert ungleich Null. Wenn die Verbindung erfolgreich ist, wird der Zähler auf Null gesetzt.
	affinitymgrExternalRcpConnRCPConnEvents .1.3.6.1.4.1.3530.8.7.145.100.20 Wenn eine Verbindung hergestellt ist, sollte sie bestehen bleiben. Achten Sie	

Gruppe	Tabelle	Zähler
	darauf, ob es zahlreiche Verbindungs-/Neuverbindungsereignisse gibt, und untersuchen Sie ggf., warum die Verbindung nicht bestehen bleibt.	
	affinitymgrExternalRcpConnRCPConnEventsConnectEvent .1.3.6.1.4.1.3530.8.7.145.100.20.2 Trap	
	affinitymgrExternalRcpConnRCPConnEventsDisconnectEvent .1.3.6.1.4.1.3530.8.7.145.100.20.3 Trap	
	affinitymgrExternalRcpConnRCPConnProxyTable .1.3.6.1.4.1.3530.8.7.145.100.30	affinitymgrExternalRcpConnRCPConnProxyTableHost .1.3.6.1.4.1.3530.8.7.145.100.30.1.2 Oktettzeichenfolge Aktiver Proxy-Inhaltsserver
affinitymgrServers .1.3.6.1.4.1.3530.8.7.145.120	affinitymgrServersServerStateTable .1.3.6.1.4.1.3530.8.7.145.120.30	affinitymgrServersServerStateTableNumUsers .1.3.6.1.4.1.3530.8.7.145.120.30.1.6 Zahl der jedem Server zugewiesenen Benutzer, indiziert nach Server-ID Ganze Zahl

BlackBerry MDS Connection Service

Gruppe	Tabelle	Zähler
mdscsProcess .1.3.6.1.4.1.3530.8.7.40.5	mdscsProcInfoTable .1.3.6.1.4.1.3530.8.7.40.5.2	mdscsProcInfoTablePID .1.3.6.1.4.1.3530.8.7.40.5.2.1.1 Ganze Zahl Numerischer Bezeichner für den Prozess

Gruppe	Tabelle	Zähler
mdscsStatistics .1.3.6.1.4.1.3530.8.7.40.20	mdscsStatsTable .1.3.6.1.4.1.3530.8.7.40.20.5	mdscsStatsTableProcQLen .1.3.6.1.4.1.3530.8.7.40.20.5.1.4 Counter64 Zahl der in der Verarbeitungswarteschlange ausstehenden Transaktionen
mdscsEvents .1.3.6.1.4.1.3530.8.7.40.30	mdscsEventsServiceStartEvent .1.3.6.1.4.1.3530.8.7.40.30.2 Trap	
	mdscsEventsServiceStopEvent .1.3.6.1.4.1.3530.8.7.40.30.3 Trap	
mdscsMDSStats .1.3.6.1.4.1.3530.8.7.40.40	mdscsMDSSummaryTable .1.3.6.1.4.1.3530.8.7.40.40.15	mdscsMDSSummaryTableRefusedPackets .1.3.6.1.4.1.3530.8.7.40.40.15.1.6 Counter64 Zahl der vom BlackBerry Dispatcher abgelehnten Pakete
		mdscsMDSSummaryTableInvalidPackets .1.3.6.1.4.1.3530.8.7.40.40.15.1.8 Counter64 Zahl der an den BlackBerry Dispatcher gesendeten ungültigen Pakete
		mdscsMDSSummaryTableExpiredPackets .1.3.6.1.4.1.3530.8.7.40.40.15.1.9 Counter64 Zahl der abgelaufenen IPPP-Pakete
		mdscsMDSSummaryTableTimedoutConnections

Gruppe	Tabelle	Zähler
		.1.3.6.1.4.1.3530.8.7.40.40.15.1.14 Counter64 Zahl der Push-Verbindungen, bei denen eine Bereitstellung nicht innerhalb des Standard-Timeouts erfolgen konnte. Dieser Zähler wird nur für Push-Verbindungen gemeldet, für die kein bestimmtes Bereitstellungs-Timeout gilt.
		mdscsMDSSummaryTableRefusedConnections .1.3.6.1.4.1.3530.8.7.40.40.15.1.15 Counter64 Zahl der abgelehnten IPPP-Verbindungen
		mdscsMDSSummaryTableSrpsuccess .1.3.6.1.4.1.3530.8.7.40.40.15.1.16 Counter64 Zahl der erfolgreichen SRP-Verbindungen mit dem BlackBerry Dispatcher.
		mdscsMDSSummaryTableSrpfailure .1.3.6.1.4.1.3530.8.7.40.40.15.1.18 Counter64 Zahl der fehlerhaften SRP-Verbindungen mit dem BlackBerry Dispatcher.
mdscsMDSAdvancedStats .1.3.6.1.4.1.3530.8.7.40.70	mdscsRatesTable .1.3.6.1.4.1.3530.8.7.40.70.5	mdscsRatesTableSocketConnectionFailedCount .1.3.6.1.4.1.3530.8.7.40.70.5.1.34 counter64 Zahl der ausgehenden TCP-Socket-Verbindungen, die nicht geöffnet werden konnten

Gruppe	Tabelle	Zähler
		mdscsRatesTableMaxSocketConnections .1.3.6.1.4.1.3530.8.7.40.70.5.1.36 Counter64 Zahl der ausgehenden TCP-Socket-Verbindungen, die während des vorherigen Berichtsintervalls offen/aktiv waren
		mdscsRatesTableSocketConnectionSuccessCount .1.3.6.1.4.1.3530.8.7.40.70.5.1.38 Counter64 Zahl der ausgehenden TCP-Socket-Verbindungen, die während des vorherigen Berichtsintervalls erfolgreich geöffnet wurden
		mdscsRatesTableSocketDisconnectionCount .1.3.6.1.4.1.3530.8.7.40.70.5.1.40 Counter64 Zahl der ausgehenden TCP-Socket-Verbindungen, die während des vorherigen Berichtsintervalls erfolgreich geschlossen wurden
		mdscsRatesTableMessageSentCount .1.3.6.1.4.1.3530.8.7.40.70.5.1.42 Counter64 Zahl der über ausgehende TCP-Socket-Verbindungen an externe Server gesendeten Datenpakete
		mdscsRatesTableMessageReceivedCount .1.3.6.1.4.1.3530.8.7.40.70.5.1.44

Gruppe	Tabelle	Zähler
		Counter64 Zahl der über ausgehende TCP-Socket-Verbindungen von externen Servern empfangene Datenpakete
mdscsMDSCSExtended .1.3.6.1.4.1.3530.8.7.40.80	mdscsExtendedRatesTable .1.3.6.1.4.1.3530.8.7.40.80.5	mdscsExtendedRatesTableNumActive .1.3.6.1.4.1.3530.8.7.40.80.5.1.2 Counter64 Zahl der aktiven IPPP/TCP-Verbindungen
		mdscsExtendedRatesTableBytesIn .1.3.6.1.4.1.3530.8.7.40.80.5.1.4 Counter64 Gesamtzahl der über TCP-Verbindungen empfangenen Bytes (in KB)
		mdscsExtendedRatesTableBytesOut .1.3.6.1.4.1.3530.8.7.40.80.5.1.6 Counter64 Gesamtzahl der über TCP-Verbindungen gesendeten Bytes (in KB)
		mdscsExtendedRatesTableConnectionErrors .1.3.6.1.4.1.3530.8.7.40.80.5.1.8 Counter64 Zahl der Socket-Verbindungsfehler
mdscsDatabaseConn .1.3.6.1.4.1.3530.8.7.40.90	mdscsDatabaseConnBaseConfigTable .1.3.6.1.4.1.3530.8.7.40.90.5	mdscsDatabaseConnBaseConfigTableEndB .1.3.6.1.4.1.3530.8.7.40.90.5.1.6 Oktettzeichenfolge Namen der Verbindungsendpunkte Name der BES12-Datenbank

Gruppe	Tabelle	Zähler
	mdscsDatabaseConnConfigTable .1.3.6.1.4.1.3530.8.7.40.90.10	mdscsDatabaseConnConfigTableConnParams .1.3.6.1.4.1.3530.8.7.40.90.10.1.2 Oktettzeichenfolge Für die Verbindung mit der BES12-Datenbank verwendete Parameter
	mdscsDatabaseConnConnectionStatsTable .1.3.6.1.4.1.3530.8.7.40.90.15	mdscsDatabaseConnConnectionStatsTableConnected .1.3.6.1.4.1.3530.8.7.40.90.15.1.2 Ganze Zahl Gibt an, ob die Verbindung hergestellt wurde.
	mdscsDatabaseConnEvents .1.3.6.1.4.1.3530.8.7.40.90.20	
	mdscsDatabaseConnEventsConnectEvent .1.3.6.1.4.1.3530.8.7.40.90.20.2 Trap	
	mdscsDatabaseConnEventsDisconnectEvent .1.3.6.1.4.1.3530.8.7.40.90.20.3 Trap	
mdscsDispatcherConn .1.3.6.1.4.1.3530.8.7.40.110	mdscsDispatcherConnConnectionStatsTable .1.3.6.1.4.1.3530.8.7.40.110.10	mdscsDispatcherConnConnectionStatsTableConnected .1.3.6.1.4.1.3530.8.7.40.110.10.1.2 Ganze Zahl Gibt an, ob die Verbindung hergestellt wurde.
		mdscsDispatcherConnConnectionStatsTableLastConDate .1.3.6.1.4.1.3530.8.7.40.110.10.1.4

Gruppe	Tabelle	Zähler
		Ganze Zahl Zeitpunkt, zu dem die Verbindung das letzte Mal erfolgreich hergestellt wurde
	mdscsDispatcherConnEvents .1.3.6.1.4.1.3530.8.7.40.110.15	
	mdscsDispatcherConnEventsConnectEvent .1.3.6.1.4.1.3530.8.7.40.110.15.2 Trap	
	mdscsDispatcherConnEventsDisconnectEvent .1.3.6.1.4.1.3530.8.7.40.110.15.3 Trap	

BlackBerry Dispatcher

Gruppe	Tabelle	Zähler
dispatcherProcess .1.3.6.1.4.1.3530.8.7.15.5	dispatcherProcInfoTable .1.3.6.1.4.1.3530.8.7.15.5.2	dispatcherProcInfoTablePID .1.3.6.1.4.1.3530.8.7.15.5.2.1.1 Ganze Zahl Numerischer Bezeichner für den Prozess
dispatcherStatistics .1.3.6.1.4.1.3530.8.7.15.20	dispatcherDispatcherStatsTable .1.3.6.1.4.1.3530.8.7.15.20.5	dispatcherDispatcherStatsTableProcQLen .1.3.6.1.4.1.3530.8.7.15.20.5.1.4 Ganze Zahl Zahl der in der Verarbeitungswarteschlange ausstehenden Transaktionen
		dispatcherDispatcherStatsTableNumUsers .1.3.6.1.4.1.3530.8.7.15.20.5.1.6

Gruppe	Tabelle	Zähler
		Ganze Zahl Zahl der dem Dienst zugewiesenen Benutzer
		dispatcherDispatcherStatsTableBIPPWorkQueueSize .1.3.6.1.4.1.3530.8.7.15.20.5.1.8 Ganze Zahl Zahl der geschäftlichen Anforderungspakete in der Warteschlange des prozessübergreifenden BlackBerry-Protokollmoduls
dispatcherTrafficStats .1.3.6.1.4.1.3530.8.7.15.30	dispatcherTotalTrafficStatsToTable .1.3.6.1.4.1.3530.8.7.15.30.33	dispatcherTotalTrafficStatsToTableMTH .1.3.6.1.4.1.3530.8.7.15.30.33.1.2 Ganze Zahl Gesamtzahl der an alle Geräte gesendeten Nachrichten
	dispatcherTotalTrafficStatsFromTable .1.3.6.1.4.1.3530.8.7.15.30.34	dispatcherTotalTrafficStatsFromTableMFH .1.3.6.1.4.1.3530.8.7.15.30.34.1.2 Ganze Zahl Gesamtzahl der von allen Geräten gesendeten Nachrichten
dispatcherEvents .1.3.6.1.4.1.3530.8.7.15.40	dispatcherEventsServiceStartEvent .1.3.6.1.4.1.3530.8.7.15.40.2 Trap	
	dispatcherEventsServiceStopEvent .1.3.6.1.4.1.3530.8.7.15.40.3 Trap	
dispatcherDatabaseConn	dispatcherDatabaseConnBaseConfigTable	dispatcherDatabaseConnBaseConfigTableEndB

Gruppe	Tabelle	Zähler
.1.3.6.1.4.1.3530.8.7.15.90	.1.3.6.1.4.1.3530.8.7.15.90.5	.1.3.6.1.4.1.3530.8.7.15.90.5.1.6 Oktettzeichenfolge Namen der Verbindungsendpunkte
	dispatcherDatabaseConnConfigTable .1.3.6.1.4.1.3530.8.7.15.90.10	dispatcherDatabaseConnConfigTableConnParams .1.3.6.1.4.1.3530.8.7.15.90.10.1.2 Oktettzeichenfolge Für die Verbindung mit der BES12-Datenbank verwendete Parameter
	dispatcherDatabaseConnConnectionStatsTable .1.3.6.1.4.1.3530.8.7.15.90.15	dispatcherDatabaseConnConnectionStatsTableConnected .1.3.6.1.4.1.3530.8.7.15.90.15.1.2 Ganze Zahl Gibt an, ob die Verbindung hergestellt wurde.
		dispatcherDatabaseConnConnectionStatsTableLastConDate .1.3.6.1.4.1.3530.8.7.15.90.15.1.4 Ganze Zahl Zeitpunkt, zu dem die Verbindung das letzte Mal erfolgreich hergestellt wurde
		dispatcherDatabaseConnConnectionStatsTableLastErrCode .1.3.6.1.4.1.3530.8.7.15.90.15.1.8 Ganze Zahl Fehlercode des letzten Verbindungsfehlers. Weitere Informationen enthalten die Protokolldateien.
		dispatcherDatabaseConnConnectionStatsTableLastErrRsn

Gruppe	Tabelle	Zähler
		.1.3.6.1.4.1.3530.8.7.15.90.15.1.6 Oktettzeichenfolge Grund des letzten Verbindungsfehlers
		dispatcherDatabaseConnConnectionStatsTableLastErrorTime .1.3.6.1.4.1.3530.8.7.15.90.15.1.10 Ganze Zahl Zeitpunkt des letzten Fehlschlagens der Verbindung
		dispatcherDatabaseConnConnectionStatsTableNumTrans .1.3.6.1.4.1.3530.8.7.15.90.15.1.12 Ganze Zahl Zahl der an die BlackBerry Configuration Database gesendeten Transaktionen
		dispatcherDatabaseConnConnectionStatsTableAvgRspTime .1.3.6.1.4.1.3530.8.7.15.90.15.1.14 Ganze Zahl Durchschnittliche Antwortzeit der Verbindung
		dispatcherDatabaseConnConnectionStatsTableErrs .1.3.6.1.4.1.3530.8.7.15.90.15.1.16 Ganze Zahl Zahl der bei der Datenbankverbindung aufgetretenen Fehler
	dispatcherDatabaseConnEvents .1.3.6.1.4.1.3530.8.7.15.90.20	
	dispatcherDatabaseConnEventsConnectEvent	

Gruppe	Tabelle	Zähler
	.1.3.6.1.4.1.3530.8.7.15.90.20.2 Trap	
	dispatcherDatabaseConnEventsDisconnectEvent .1.3.6.1.4.1.3530.8.7.15.90.20.3 Trap	
dispatcherInternalSrvConn .1.3.6.1.4.1.3530.8.7.15.110	dispatcherInternalSrvConnRCPConnStatsTable .1.3.6.1.4.1.3530.8.7.15.110.15	dispatcherInternalSrvConnRCPConnStatsTableConnected .1.3.6.1.4.1.3530.8.7.15.110.15.1.2 Ganze Zahl Gibt an, ob die Verbindung hergestellt wurde.
		dispatcherInternalSrvConnRCPConnStatsTableTransQLen .1.3.6.1.4.1.3530.8.7.15.110.15.1.14 Ganze Zahl Länge der Übertragungswarteschlange (Zahl der Transaktionen, die auf die Übertragung warten)
		dispatcherInternalSrvConnRCPConnStatsTableBytesReceived .1.3.6.1.4.1.3530.8.7.15.110.15.1.16 Counter64 Über die RCP-Verbindung empfangene Bytes
		dispatcherInternalSrvConnRCPConnStatsTableBytesSent .1.3.6.1.4.1.3530.8.7.15.110.15.1.18 Counter64 Über die RCP-Verbindung gesendete Bytes

Gruppe	Tabelle	Zähler
		dispatcherInternalSrvConnRCPConnStatsTableReceiveTransactions .1.3.6.1.4.1.3530.8.7.15.110.15.1.20 Counter64 Zahl der über die RCP-Verbindung erfolgten Empfangsvorgänge
		dispatcherInternalSrvConnRCPConnStatsTableSendTransactions .1.3.6.1.4.1.3530.8.7.15.110.15.1.22 Counter64 Zahl der über die RCP-Verbindung erfolgten Sendevorgänge
	dispatcherInternalSrvConnRCPConnEvents .1.3.6.1.4.1.3530.8.7.15.110.20	
	dispatcherInternalSrvConnRCPConnEventsConnectEvent .1.3.6.1.4.1.3530.8.7.15.110.20.2 Trap	
	dispatcherInternalSrvConnRCPConnEventsDisconnectEvent .1.3.6.1.4.1.3530.8.7.15.110.20.3 Trap	
dispatcherRcpConn .1.3.6.1.4.1.3530.8.7.15.120	dispatcherRcpConnRCPConnStatsTable .1.3.6.1.4.1.3530.8.7.15.120.15	dispatcherRcpConnRCPConnStatsTableLastModTime .1.3.6.1.4.1.3530.8.7.15.120.15.1.1 Ganze Zahl Zeitpunkt der letzten Änderung eines Wertesatzes
		dispatcherRcpConnRCPConnStatsTableConnected

Gruppe	Tabelle	Zähler
		.1.3.6.1.4.1.3530.8.7.15.120.15.1.2 Ganze Zahl Gibt an, ob die Verbindung hergestellt wurde.
		dispatcherRcpConnRCPConnStatsTable LastConDate .1.3.6.1.4.1.3530.8.7.15.120.15.1.4 Ganze Zahl Zeitpunkt, zu dem die Verbindung das letzte Mal erfolgreich hergestellt wurde
		dispatcherRcpConnRCPConnStatsTable LastErrCode .1.3.6.1.4.1.3530.8.7.15.120.15.1.6 Ganze Zahl Fehlercode des letzten Verbindungsfehlers. Weitere Informationen enthalten die Protokolldateien.
		dispatcherRcpConnRCPConnStatsTableT ransQLen .1.3.6.1.4.1.3530.8.7.15.120.15.1.14 Ganze Zahl Länge der Übertragungswarteschlange (Zahl der Transaktionen, die auf die Übertragung warten)
		dispatcherRcpConnRCPConnStatsTable BytesReceived .1.3.6.1.4.1.3530.8.7.15.120.15.1.16 Counter64 Über die RCP-Verbindung empfangene Bytes

Gruppe	Tabelle	Zähler
		dispatcherRcpConnRCPConnStatsTable BytesSent .1.3.6.1.4.1.3530.8.7.15.120.15.1.18 Counter64 Über die RCP-Verbindung gesendete Bytes
		dispatcherRcpConnRCPConnStatsTable ReceiveTransactions .1.3.6.1.4.1.3530.8.7.15.120.15.1.20 Counter64 Zahl der über die RCP-Verbindung erfolgten Empfangsvorgänge
		dispatcherRcpConnRCPConnStatsTable SendTransactions .1.3.6.1.4.1.3530.8.7.15.120.15.1.22 Counter64 Zahl der über die RCP-Verbindung erfolgten Sendevorgänge
	dispatcherRcpConnRCPConnEvents .1.3.6.1.4.1.3530.8.7.15.120.20	
	dispatcherRcpConnRCPConnEventsConnectEvent .1.3.6.1.4.1.3530.8.7.15.120.20.2 Trap	
	dispatcherRcpConnRCPConnEventsDisconnectEvent .1.3.6.1.4.1.3530.8.7.15.120.20.3 Trap	

SNMP-Zähler für BES12 Core

Die folgenden Tabellen enthalten Informationen über einige wichtige SNMP-Zähler zur Überwachung der Leistung und Aktivität von BES12 Core:

Überwachung

Gruppe	Tabelle	Zähler
monitors .1.3.6.1.4.1.3530.8.1.1.2	reconciliationmonitor .1.3.6.1.4.1.3530.8.1.1.2.1	reconciliationmonitorReconciliationRequestCount .1.3.6.1.4.1.3530.8.1.1.2.1.1 Unsigned32 Kumulative Zahl der Synchronisierungsanforderungen
		reconciliationmonitorReconciliationCurrentTime .1.3.6.1.4.1.3530.8.1.1.2.1.4 Gauge32 Zeitdauer des letzten Synchronisierungsprozesses
		reconciliationmonitorReconciliationTotalTime .1.3.6.1.4.1.3530.8.1.1.2.1.5 Unsigned32 Zeitdauer aller Synchronisierungsprozesse
	coretobcpconnectionmonitor .1.3.6.1.4.1.3530.8.1.1.2.100	coretobcpconnectionmonitorConnectionCount .1.3.6.1.4.1.3530.8.1.1.2.100.1 Unsigned32 Zahl der Verbindungen zwischen BES12 Core und der BlackBerry Infrastructure
		coretobcpconnectionmonitorConnectionFailureCount

Gruppe	Tabelle	Zähler
		.1.3.6.1.4.1.3530.8.1.1.2.100.2 Unsigned32 Zahl der fehlerhaften Verbindungen zwischen BES12 Core und der BlackBerry Infrastructure
		coretobcpconnectionmonitorTotalProcessingTime .1.3.6.1.4.1.3530.8.1.1.2.100.3 Gauge32
		coretobcpconnectionmonitorBytesFromBcp .1.3.6.1.4.1.3530.8.1.1.2.100.4 Gauge32 Zahl der aus der BlackBerry Infrastructure empfangenen Bytes insgesamt
		coretobcpconnectionmonitorBytesToBcp .1.3.6.1.4.1.3530.8.1.1.2.100.5 Gauge32 Zahl der an die BlackBerry Infrastructure gesendeten Bytes insgesamt

Workflow

Gruppe	Tabelle	Zähler
wffqueues .1.3.6.1.4.1.3530.8.1.1.3	androidnotificationqueue .1.3.6.1.4.1.3530.8.1.1.3.1	androidnotificationqueueAddOperations .1.3.6.1.4.1.3530.8.1.1.3.1.1 Unsigned32 Zahl der Hinzufügungen zur Warteschlange
		androidnotificationqueueSize

Gruppe	Tabelle	Zähler
		.1.3.6.1.4.1.3530.8.1.1.3.1.2 Unsigned32 Aktuelle Größe der Warteschlange
		androidnotificationqueueTakeOperations .1.3.6.1.4.1.3530.8.1.1.3.1.3 Unsigned32 Zahl der Entnahmen aus der Warteschlange
	applenotificationqueue .1.3.6.1.4.1.3530.8.1.1.3.2	applenotificationqueueAddOperations .1.3.6.1.4.1.3530.8.1.1.3.2.1 Unsigned32 Zahl der Hinzufügungen zur Warteschlange
		applenotificationqueueSize .1.3.6.1.4.1.3530.8.1.1.3.2.2 Unsigned32 Aktuelle Größe der Warteschlange
		applenotificationqueueTakeOperations .1.3.6.1.4.1.3530.8.1.1.3.2.3 Unsigned32 Zahl der Entnahmen aus der Warteschlange
	bbnotificationqueue .1.3.6.1.4.1.3530.8.1.1.3.4	bbnotificationqueueAddOperations .1.3.6.1.4.1.3530.8.1.1.3.4.1 Unsigned32 Zahl der Hinzufügungen zur Warteschlange
		bbnotificationqueueSize .1.3.6.1.4.1.3530.8.1.1.3.4.2

Gruppe	Tabelle	Zähler
		Unsigned32 Aktuelle Größe der Warteschlange
		bbnotificationqueueTakeOperations .1.3.6.1.4.1.3530.8.1.1.3.4.3 Unsigned32 Zahl der Entnahmen aus der Warteschlange
	devicerestqueue .1.3.6.1.4.1.3530.8.1.1.3.7	devicerestqueueAddOperations .1.3.6.1.4.1.3530.8.1.1.3.7.1 Unsigned32 Zahl der Hinzufügungen zur Warteschlange
		devicerestqueueSize .1.3.6.1.4.1.3530.8.1.1.3.7.2 Unsigned32 Aktuelle Größe der Warteschlange
		devicerestqueueTakeOperations .1.3.6.1.4.1.3530.8.1.1.3.7.3 Unsigned32 Zahl der Entnahmen aus der Warteschlange
	downloadrestqueue .1.3.6.1.4.1.3530.8.1.1.3.9	downloadrestqueueAddOperations .1.3.6.1.4.1.3530.8.1.1.3.9.1 Unsigned32 Zahl der Hinzufügungen zur Warteschlange
		downloadrestqueueSize .1.3.6.1.4.1.3530.8.1.1.3.9.2 Unsigned32

Gruppe	Tabelle	Zähler
		Aktuelle Größe der Warteschlange
		downloadrestqueueTakeOperations .1.3.6.1.4.1.3530.8.1.1.3.9.3 Unsigned32 Zahl der Entnahmen aus der Warteschlange

SNMP-Zähler für BlackBerry Secure Connect Plus

Die folgende Tabelle enthält Informationen über einige wichtige SNMP-Zähler zur Überwachung der Leistung und Aktivität von BlackBerry Secure Connect Plus:

Überwachung

Gruppe	Überwachungspunkte	Zähler
monitors .1.3.6.1.4.1.3530.8.2.1.2	Ptsservicemonitor .1.3.6.1.4.1.3530.8.2.1.2.1 Überwachungspunkte des BlackBerry Secure Connect Plus-Diensts	ptsservicemonitorptsTunnelCount .1.3.6.1.4.1.3530.8.2.1.2.1.1 GAUGE32 Gesamtzahl der Gerätetunnel seit dem Start
		ptsservicemonitorcountOfCurrentPtsTunnels .1.3.6.1.4.1.3530.8.2.1.2.1.2 GAUGE32 Zahl der aktuellen Gerätetunnel
		ptsservicemonitorptsBytesSentTotal .1.3.6.1.4.1.3530.8.2.1.2.1.7 GAUGE32 An den Client gesendete BSCP-Bytes insgesamt

Gruppe	Überwachungspunkte	Zähler
		ptsservicemonitorptsBytesReceivedTotal .1.3.6.1.4.1.3530.8.2.1.2.1.8 GAUGE32 Von Clients empfangene BSCP-Pakete
		ptsservicemonitorptsBytesDroppedTotal .1.3.6.1.4.1.3530.8.2.1.2.1.9 GAUGE32 Verlorene BSCP-Bytes insgesamt
		ptsservicemonitoractiveTurnAllocations .1.3.6.1.4.1.3530.8.2.1.2.1.10 GAUGE32 Zahl der derzeit aktiven Verbindungen mit der BlackBerry Infrastructure
		coretobcpconnectionmonitorBytesFrom Bcp .1.3.6.1.4.1.3530.8.1.1.2.100.4 Gauge32 Zahl der aus der BlackBerry Infrastructure empfangenen Bytes insgesamt
		ptsservicemonitorptsPacketsDroppedTot al .1.3.6.1.4.1.3530.8.2.1.2.1.11 GAUGE32 Verlorene BSCP-Pakete insgesamt

Profileinstellungen

Zeigen Sie detaillierte Beschreibungen der Profileinstellungen an, um Hilfe bei der Konfiguration von E-Mail, SCEP, Wi-Fi und VPN-Profilen zu erhalten.

Multiplatform

E-Mail-Profileinstellungen

30

Sie können eine Variable in einem beliebigen Textfeld der Profileinstellungen verwenden, um einen Wert zu referenzieren, statt den tatsächlichen Wert anzugeben. BES12 unterstützt vordefinierte Standardvariablen sowie von Ihnen festgelegte benutzerdefinierte Variablen. E-Mail-Profile werden auf den folgenden Gerätetypen unterstützt:

- BlackBerry 10
- iOS
- Android
- Windows Phone

In einigen Fällen wird die erforderliche Mindestversion des Gerätebetriebssystems zur Unterstützung einer Einstellung nicht von BES12 unterstützt. Weitere Informationen zu unterstützten Versionen finden Sie in der Kompatibilitätsmatrix in der Dokumentation zu Installation und Upgrade.

Allgemein: E-Mail-Profileinstellungen

Allgemein: E-Mail-Profileinstellung	Beschreibung
Domänenname	Diese Einstellung legt den Domänenname des Mailservers fest.
E-Mail-Adresse	Diese Einstellung legt die E-Mail-Adresse des Benutzers fest. Wenn das Profil für mehrere Benutzer gilt, können Sie die %UserEmailAddress%-Variable verwenden.
Hostname oder IP-Adresse	Diese Einstellung legt den Hostnamen oder die IP-Adresse Mailservers fest.
Benutzername	Diese Einstellung legt den Benutzernamen des Benutzers fest. Wenn das Profil für mehrere Benutzer gilt, können Sie die %UserName%-Variable verwenden.
Automatische Gatekeeping-Server	Diese Einstellung legt die Microsoft Exchange-Server fest, die mit automatischem Gatekeeping für Geräte arbeiten können. Wenn das E-Mail-Konto eines Benutzers auf einem bestimmten Server liegt, der Benutzer ein BlackBerry 10-, iOS-, Windows Phone- oder Android-Gerät mit der Aktivierungsart Geschäftlich und persönlich – vollständige Kontrolle oder Geschäftlich und persönlich – Benutzer-Datenschutz aktiviert und das Gerät die Sicherheitsrichtlinien Ihrer Organisation erfüllt, wird das Gerät automatisch zu der Liste der zulässigen Geräte in Microsoft Exchange hinzugefügt. Diese Geräte werden automatisch aus der Liste der zulässigen Geräte entfernt, wenn eine nicht zugewiesene App installiert wird, wenn das Gerät gegen die Einstellungen im zugewiesenen Kompatibilitätsprofil verstößt oder wenn das Gerät deaktiviert wird.

Allgemein: E-Mail-Profileinstellung	Beschreibung
	Vorhandenen Benutzerkonten oder Gruppen müssen Sie das mit Gatekeeping konfigurierte E-Mail-Profil manuell erneut zuweisen, um diese Funktion zu implementieren. Wenn Sie automatisches Gatekeeping einrichten, muss als „Profiltyp“ auf BlackBerry 10- und Windows Phone-Geräten „Exchange ActiveSync“ eingestellt werden.

BlackBerry 10: E-Mail-Profileinstellungen

BlackBerry 10: E-Mail-Profileinstellung	Beschreibung
Kontoname	Diese Einstellung legt den Namen des geschäftlichen E-Mail-Kontos fest, der im BlackBerry Hub und in den Geräteeinstellungen angezeigt wird. Sie können eine Variable wie etwa „%UserEmailAddress%“ verwenden.
Port	Diese Einstellung legt den Port fest, der für die Verbindung zum Mailserver verwendet wird.
Übermittlungseinstellungen	
Profiltyp	Diese Einstellung legt fest, ob das Profil Exchange ActiveSync oder IBM Notes Traveler unterstützen soll. Mögliche Werte: • Exchange ActiveSync • IBM Notes Traveler Der Standardwert ist „Exchange ActiveSync“.
SyncML-Server	Diese Einstellung legt den FQDN des IBM Notes Traveler-Servers fest, den ein BlackBerry 10-Gerät verwenden kann, um ToDo-Daten zu synchronisieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Profiltyp“ auf „IBM Notes Traveler“ gesetzt ist.
SyncML-Port	Diese Einstellung legt den Port des Notes Traveler-Servers fest, den ein BlackBerry 10-Gerät verwenden kann, um ToDo-Daten zu synchronisieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Profiltyp“ auf „IBM Notes Traveler“ gesetzt ist.
SSL für SyncML verwenden	Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät eine SSL-Verbindung zum Notes Traveler-Server aufbauen muss.

BlackBerry 10: E-Mail-Profileinstellung	Beschreibung
	Diese Einstellung ist nur dann gültig, wenn die Einstellung „Profiltyp“ auf „IBM Notes Traveler“ gesetzt ist.
Push aktiviert	Diese Einstellung legt fest, ob der Mailserver E-Mail-Nachrichten mithilfe von Push auf ein BlackBerry 10-Gerät übertragen kann.
Zeitraum zwischen Synchronisierungen	Diese Einstellung legt fest, wie häufig ein BlackBerry 10-Gerät neue E-Mail-Nachrichten vom Mailserver abruft. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Push aktiviert“ nicht ausgewählt ist. Mögliche Werte: • Manuell • 5 Minuten • 15 Minuten • 30 Minuten • 1 Stunde • 2 Stunden • 4 Stunden • 24 Stunden Der Standardwert ist „15 Minuten“.
Tage für Synchronisierung	Diese Einstellung legt fest, für wie viele Tage in der Vergangenheit E-Mail-Nachrichten und Terminplanerdaten auf ein BlackBerry 10-Gerät synchronisiert werden sollen. Mögliche Werte: • 1 Tag • 3 Tage • 7 Tage • 14 Tage • 1 Monat • Unbegrenzt Der Standardwert ist „1 Monat“.
Beim Roaming manuelle Synchronisierung initiieren	Diese Einstellung legt fest, ob ein Benutzer beim Roaming eine Synchronisierung zwischen einem BlackBerry 10-Gerät und dem Mailserver starten muss.

BlackBerry 10: E-Mail-Profileinstellung	Beschreibung
SSL verwenden	Diese Einstellung legt fest, ob ein Gerät SSL verwenden muss, um eine Verbindung zum Mailserver aufzubauen.
Kalendersynchronisierung	Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät Kalendereinträge mit dem Mailserver synchronisiert.
Kontaktsynchronisierung	Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät Kontakte mit dem Mailserver synchronisiert.
E-Mail-Synchronisierung	Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät E-Mail-Nachrichten mit dem Mailserver synchronisiert.
Notizensynchronisierung	Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät Notizen mit dem Mailserver synchronisiert. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Profiltyp“ auf „Exchange ActiveSync“ gesetzt ist.
Aufgabensynchronisierung	Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät Aufgabendaten mit dem Mailserver synchronisiert. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Profiltyp“ auf „Exchange ActiveSync“ gesetzt ist.
ToDo-Synchronisierung	Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät die ToDo-Daten mit Notes Traveler synchronisiert. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Profiltyp“ auf „IBM Notes Traveler“ gesetzt ist.
Sichere E-Mail-Einstellungen	
Standardverschlüsselung für ausgehende Nachrichten vorschlagen	Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät die Standardverschlüsselung (z. B. nur Text, signieren, verschlüsseln oder signieren und verschlüsseln) für alle ausgehenden E-Mail-Nachrichten vorschlägt. Wenn diese Einstellung auf „Zulassen“ gesetzt ist, kann ein Benutzer entscheiden, ob das Gerät die Standardverschlüsselung oder eine Verschlüsselung basierend auf dem Nachrichtenverlauf vorschlägt. Wenn diese Einstellung auf „Erforderlich“ gesetzt ist, schlägt das Gerät die Standardverschlüsselung vor. Wenn diese Einstellung auf „Nicht zulassen“ gesetzt ist, schlägt das Gerät die Verschlüsselung basierend auf dem Nachrichtenverlauf vor. Mögliche Werte: • Zulassen

BlackBerry 10: E-Mail-Profileinstellung	Beschreibung
	• Erforderlich • Nicht zulassen Der Standardwert ist „Zulassen“. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.
S/MIME-Einstellungen	
S/MIME-Unterstützung	Diese Einstellung legt fest, ob S/MIME auf einem BlackBerry 10-Gerät aktiviert ist. Wenn diese Einstellung auf „Zulassen“ gesetzt ist, kann ein Benutzer entscheiden, ob S/MIME-Schutz auf dem Gerät aktiviert oder nicht aktiviert werden soll. Wenn diese Einstellung auf „Erforderlich“ gesetzt ist, ist S/MIME-Schutz auf dem Gerät aktiviert, und der Benutzer kann ihn nicht deaktivieren. Wenn diese Einstellung auf „Nicht zulassen“ gesetzt ist, ist S/MIME-Schutz auf dem Gerät deaktiviert, und der Benutzer kann ihn nicht aktivieren. Um verschlüsselte E-Mail-Nachrichten senden zu können, muss der Benutzer den öffentlichen Schlüssel des Empfängers auf seinem Gerät beziehungsweise der Smartcard zur Verfügung haben. Um digital signierte E-Mail-Nachrichten senden zu können, muss der private Schlüssel des Benutzers auf dem Gerät beziehungsweise der Smartcard verfügbar sein. Diese Einstellung hat höhere Priorität als die Einstellungen „Digital signierte S/MIME-Nachrichten“ und „Verschlüsselte S/MIME-Nachrichten“. Diese Einstellung betrifft die Einstellung „PGP-Support“. Wenn diese Einstellung auf „Erforderlich“ gesetzt ist, muss die Einstellung „PGP-Support“ auf „Nicht zulassen“ gesetzt werden. Mögliche Werte: • Zulassen • Erforderlich • Nicht zulassen Der Standardwert ist „Zulassen“.
Digital signierte S/MIME-Nachrichten	Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät ausgehende E-Mail-Nachrichten mit digitaler Signatur sendet. Wenn diese Einstellung auf „Zulassen“ gesetzt ist, kann der Benutzer entscheiden, ob er ausgehende E-Mail-Nachrichten digital signieren möchte. Wenn diese Einstellung auf „Erforderlich“ gesetzt ist, muss der Benutzer ausgehende E-Mail-Nachrichten digital signieren. Wenn diese Einstellung auf „Nicht zulassen“ gesetzt ist, kann der Benutzer ausgehende E-Mail-Nachrichten nicht digital signieren.

BlackBerry 10: E-Mail-Profileinstellung	Beschreibung
	Um digital signierte E-Mail-Nachrichten senden zu können, muss der private Schlüssel des Benutzers auf dem Gerät beziehungsweise der Smartcard verfügbar sein. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME-Unterstützung“ auf „Zulassen“ oder „Erforderlich“ gesetzt ist. Wenn die Einstellung „S/MIME-Unterstützung“ auf „Erforderlich“ gesetzt ist und sowohl diese Einstellung als auch die Einstellung „Verschlüsselte S/MIME-Nachrichten“ auf „Nicht zulassen“ gesetzt sind, werden die Einstellung „Verschlüsselte S/MIME-Nachrichten“ und diese Einstellung ignoriert, und die Standardeinstellung „Zulassen“ wird für beide Einstellungen verwendet. Mögliche Werte: • Zulassen • Erforderlich • Nicht zulassen Der Standardwert ist „Zulassen“.
Verschlüsselte S/MIME-Nachrichten	Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät ausgehende E-Mail-Nachrichten mit S/MIME-Verschlüsselung verschlüsselt. Wenn diese Einstellung auf „Zulassen“ gesetzt ist, kann der Benutzer entscheiden, ob ausgehende E-Mail-Nachrichten verschlüsselt oder nicht verschlüsselt werden sollen. Wenn diese Einstellung auf „Erforderlich“ gesetzt ist, muss der Benutzer ausgehende E-Mail-Nachrichten verschlüsseln. Wenn diese Einstellung auf „Nicht zulassen“ gesetzt ist, kann der Benutzer ausgehende E-Mail-Nachrichten nicht verschlüsseln. Um verschlüsselte E-Mail-Nachrichten senden zu können, muss der Benutzer den öffentlichen Schlüssel des Empfängers auf seinem Gerät beziehungsweise der Smartcard zur Verfügung haben. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME-Unterstützung“ auf „Zulassen“ oder „Erforderlich“ gesetzt ist. Wenn die Einstellung „S/MIME-Unterstützung“ auf „Erforderlich“ gesetzt ist und sowohl diese Einstellung als auch die Einstellung „Digital signierte S/MIME-Nachrichten“ auf „Nicht zulassen“ gesetzt sind, werden die Einstellung „Digital signierte S/MIME-Nachrichten“ und diese Einstellung ignoriert, und die Standardeinstellung „Zulassen“ wird für beide Einstellungen verwendet. Mögliche Werte: • Zulassen • Erforderlich • Nicht zulassen

BlackBerry 10: E-Mail-Profileinstellung	Beschreibung
	Der Standardwert ist „Zulassen“.
Verschlüsselungsalgorithmen	Diese Einstellung gibt die Verschlüsselungsalgorithmen an, mit denen ein BlackBerry 10-Gerät S/MIME-geschützte E-Mail-Nachrichten verschlüsseln kann. Mögliche Werte: • AES (256-Bit) • AES (192-Bit) • AES (128-Bit) • Triple DES • RC2 Der Standardwert ist ein Nullwert.
PGP-Einstellungen	
PGP-Unterstützung	Diese Einstellung legt fest, ob PGP-Schutz auf einem BlackBerry 10-Gerät aktiviert ist. Wenn diese Einstellung auf „Zulassen“ gesetzt ist, kann ein Benutzer entscheiden, ob PGP-Schutz auf dem Gerät aktiviert oder nicht aktiviert werden soll. Wenn diese Einstellung auf „Erforderlich“ gesetzt ist, ist PGP-Schutz auf dem Gerät aktiviert, und der Benutzer kann ihn nicht deaktivieren. Wenn diese Einstellung auf „Nicht zulassen“ gesetzt ist, ist PGP-Schutz auf dem Gerät deaktiviert, und der Benutzer kann ihn nicht aktivieren. Um verschlüsselte E-Mail-Nachrichten senden zu können, muss der Benutzer den öffentlichen Schlüssel des Empfängers auf seinem Gerät zur Verfügung haben. Um digital signierte E-Mail-Nachrichten senden zu können, muss der private Schlüssel des Benutzers auf dem Gerät verfügbar sein. Die Einstellung „S/MIME-Unterstützung“ betrifft diese Einstellung. Wenn die Einstellung „S/MIME-Unterstützung“ auf „Erforderlich“ oder „Zulassen“ gesetzt und die Einstellung „Digital signierte S/MIME-Nachrichten“ oder die Einstellung„Verschlüsselte S/MIMW-Nachrichten“ auf „Erforderlich“ gesetzt ist, muss diese Einstellung auf „Nicht zulassen“ gesetzt werden. Mögliche Werte: • Zulassen • Erforderlich • Nicht zulassen Der Standardwert ist „Zulassen“. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.

BlackBerry 10: E-Mail-Profileinstellung	Beschreibung
Symantec Encryption Management Server-Adresse	Diese Einstellung legt den FQDN oder die IP-Adresse für den Symantec Encryption Management Server Ihrer Organisation fest, damit ein BlackBerry 10-Gerät bei diesem Server angemeldet werden muss, um PGP-Nachrichten senden zu können. Die Einstellung „PGP-Support“ betrifft diese Einstellung. Das Gerät verwendet diese Einstellung, wenn die Einstellung „PGP-Support“ auf „Zulassen“ oder „Erforderlich“ gesetzt ist. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.
Symantec Encryption Management Server-Anmeldemethode	Diese Einstellung legt die Methode fest, mit der sich der Benutzer eines BlackBerry 10-Gerätes beim Symantec Encryption Management Server Ihrer Organisation anmelden muss. Wenn diese Einstellung auf „E-Mail-Authentifizierung“ gesetzt ist, wird der Benutzer zur Eingabe einer E-Mail-Adresse aufgefordert. Wenn diese Einstellung auf „Microsoft Active Directory-Authentifizierung“ gesetzt ist, wird der Benutzer aufgefordert, einen Domänen-Benutzernamen und ein Kennwort einzugeben. Die Einstellung „PGP-Support“ betrifft diese Einstellung. Das Gerät verwendet diese Einstellung, wenn die Einstellung „PGP-Support“ auf „Zulassen“ oder „Erforderlich“ gesetzt ist. Mögliche Werte: • E-Mail-Authentifizierung • Microsoft Active Directory-Authentifizierung Der Standardwert ist „E-Mail-Authentifizierung“. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.
Verknüpfte Profile	
Authentifizierungstyp	Diese Einstellung legt fest, welche Art der Authentifizierung ein BlackBerry 10-Gerät verwendet, um eine Verbindung zum Mailserver aufzubauen. Mögliche Werte: • Keine • SCEP • Benutzeranmeldeinformationen Der Standardwert ist „Keine“.
Verknüpftes SCEP-Profil	Diese Einstellung legt das verknüpfte SCEP-Profil fest, mit dem der Benutzer eines BlackBerry 10-Geräts ein Client-Zertifikat für die Authentifizierung beim Mailserver anmeldet.

BlackBerry 10: E-Mail-Profileinstellung	Beschreibung
	Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „SCEP“ gesetzt ist.
Verknüpftes Profil für Benutzeranmeldeinformationen	Diese Einstellung legt das verknüpfte Profil für Benutzeranmeldeinformationen fest, mit denen der Benutzer eines BlackBerry 10-Geräts ein Client-Zertifikat für die Authentifizierung beim Mailserver erhält. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Benutzeranmeldeinformationen“ gesetzt ist. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.
Nachrichtenklassifizierung	
Nachrichtenklassifizierungsdatei (.json)	Diese Einstellung gibt die Nachrichtenklassifizierungsdatei an, die an Benutzergeräte gesendet werden soll. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.

Verwandte Informationen

Erzwingen von sicherer E-Mail mithilfe der Nachrichtenklassifizierung, auf Seite 93

S/MIME-Profil und Geräteeinstellungsabhängigkeiten

Die folgende Tabelle zeigt die Abhängigkeiten zwischen den S/MIME-Einstellungen, die Sie in BES12 konfigurieren können, und den S/MIME-Einstellungen, die Benutzer auf BlackBerry 10-Geräten konfigurieren können. Abhängig von den jeweiligen Einstellungen ändern sich die Optionen in der Dropdown-Liste „Verschlüsselung“ auf den Geräten. Geräte ignorieren den Wert einiger Einstellungen, wenn eine höhere Prioritätseinstellung (z. B. die Einstellung „S/MIME-Unterstützung“) mit dem Wert für diese Einstellung in Konflikt steht.

Einstellung „S/MIME-Unterstützung“	Einstellung „Digital signierte S/MIME-Nachrichten“	Einstellung „Verschlüsselte S/MIME-Nachrichten“	S/MIME-Einstellungen auf dem Gerät	Dropdown-Liste „Verschlüsselung“ auf dem Gerät
Zulässig	Zulässig	Zulässig	Der Benutzer kann den S/MIME-Schutz ein- oder ausschalten.	• Nur Text • Signieren (S/MIME) • Verschlüsseln (S/MIME)

Einstellung „S/MIME-Unterstützung“	Einstellung „Digital signierte S/MIME-Nachrichten“	Einstellung „Verschlüsselte S/MIME-Nachrichten“	S/MIME-Einstellungen auf dem Gerät	Dropdown-Liste „Verschlüsselung“ auf dem Gerät
				• Signieren und verschlüsseln (S/MIME)
	Zulässig	Erforderlich	S/MIME-Schutz ist eingeschaltet. Der Benutzer kann ihn nicht ausschalten.	• Verschlüsseln (S/MIME) • Signieren und verschlüsseln (S/MIME)
	Zulässig	Unzulässig	Der Benutzer kann den S/MIME-Schutz ein- oder ausschalten.	• Nur Text • Signieren (S/MIME)
	Erforderlich	Zulässig	S/MIME-Schutz ist eingeschaltet. Der Benutzer kann ihn nicht ausschalten.	• Signieren (S/MIME) • Signieren und verschlüsseln (S/MIME)
	Erforderlich	Erforderlich	S/MIME-Schutz ist eingeschaltet. Der Benutzer kann ihn nicht ausschalten.	Signieren und verschlüsseln (S/MIME)
	Erforderlich	Unzulässig	S/MIME-Schutz ist eingeschaltet. Der Benutzer kann ihn nicht ausschalten.	Signieren (S/MIME)
	Unzulässig	Zulässig	Der Benutzer kann den S/MIME-Schutz ein- oder ausschalten.	• Nur Text • Verschlüsseln (S/MIME)
	Unzulässig	Erforderlich	S/MIME-Schutz ist eingeschaltet. Der Benutzer kann ihn nicht ausschalten.	Verschlüsseln (S/MIME)

Einstellung „S/MIME-Unterstützung“	Einstellung „Digital signierte S/MIME-Nachrichten“	Einstellung „Verschlüsselte S/MIME-Nachrichten“	S/MIME-Einstellungen auf dem Gerät	Dropdown-Liste „Verschlüsselung“ auf dem Gerät
	Unzulässig	Unzulässig	Der Benutzer kann den S/MIME-Schutz ein- oder ausschalten, aber er kann Nachrichten nicht verschlüsseln oder signieren, da die erforderlichen Profile auf „Unzulässig“ eingestellt sind.	Nur Text
Erforderlich	Zulässig	Zulässig	S/MIME-Schutz ist eingeschaltet. Der Benutzer kann ihn nicht ausschalten.	• Signieren (S/MIME) • Verschlüsseln (S/MIME) • Signieren und verschlüsseln (S/MIME)
	Zulässig	Erforderlich	S/MIME-Schutz ist eingeschaltet. Der Benutzer kann ihn nicht ausschalten.	• Verschlüsseln (S/MIME) • Signieren und verschlüsseln (S/MIME)
	Zulässig	Unzulässig	S/MIME-Schutz ist eingeschaltet. Der Benutzer kann ihn nicht ausschalten.	Signieren (S/MIME)
	Erforderlich	Zulässig	S/MIME-Schutz ist eingeschaltet. Der Benutzer kann ihn nicht ausschalten.	• Signieren (S/MIME) • Signieren und verschlüsseln (S/MIME)
	Erforderlich	Erforderlich	S/MIME-Schutz ist eingeschaltet. Der Benutzer kann ihn nicht ausschalten.	Signieren und verschlüsseln (S/MIME)

Einstellung „S/MIME-Unterstützung“	Einstellung „Digital signierte S/MIME-Nachrichten“	Einstellung „Verschlüsselte S/MIME-Nachrichten“	S/MIME-Einstellungen auf dem Gerät	Dropdown-Liste „Verschlüsselung“ auf dem Gerät
	Erforderlich	Unzulässig	S/MIME-Schutz ist eingeschaltet. Der Benutzer kann ihn nicht ausschalten.	Signieren (S/MIME)
	Unzulässig	Zulässig	S/MIME-Schutz ist eingeschaltet. Der Benutzer kann ihn nicht ausschalten.	Verschlüsseln (S/MIME)
	Unzulässig	Erforderlich	S/MIME-Schutz ist eingeschaltet. Der Benutzer kann ihn nicht ausschalten.	Verschlüsseln (S/MIME)
	Unzulässig (Diese Einstellung wird ignoriert)	Unzulässig (Diese Einstellung wird ignoriert)	S/MIME-Schutz ist eingeschaltet. Der Benutzer kann ihn nicht ausschalten.	• Signieren (S/MIME) • Verschlüsseln (S/MIME) • Signieren und verschlüsseln (S/MIME)
Unzulässig	Alle Einstellungen werden ignoriert	Alle Einstellungen werden ignoriert	S/MIME-Schutz ist ausgeschaltet. Der Benutzer kann ihn nicht einschalten.	Nur Text

PGP-Profil und Geräteeinstellungsabhängigkeiten

Die folgende Tabelle zeigt die Abhängigkeiten zwischen der „PGP-Unterstützung“, die Sie in BES12 konfigurieren können, und den PGP-Einstellungen, die Benutzer auf BlackBerry 10-Geräten konfigurieren können. Abhängig von der Einstellung der „PGP-Unterstützung“ ändern sich die Optionen in der Dropdown-Liste „Verschlüsselung“ auf den Geräten. Geräte ignorieren den Wert dieser Einstellung, wenn eine höhere Prioritätseinstellung (z. B. die Einstellung „S/MIME-Unterstützung“) mit dem Wert für diese Einstellung in Konflikt steht.

Einstellung „PGP-Unterstützung“	PGP-Einstellungen auf dem Gerät	Dropdown-Liste „Verschlüsselung“ auf dem Gerät
Zulassen	Die Benutzer können den PGP-Schutz ein- oder ausschalten.	• Nur Text • Signieren (PGP)

Einstellung „PGP-Unterstützung“	PGP-Einstellungen auf dem Gerät	Dropdown-Liste „Verschlüsselung“ auf dem Gerät
		• Verschlüsseln (PGP) • Signieren und verschlüsseln (PGP)
Erforderlich	PGP-Schutz ist eingeschaltet. Der Benutzer kann ihn nicht ausschalten.	• Signieren (PGP) • Verschlüsseln (PGP) • Signieren und verschlüsseln (PGP)
Nicht zulassen	PGP-Schutz ist ausgeschaltet. Der Benutzer kann ihn nicht einschalten.	Keine Dropdown-Liste. Nur-Text wird verwendet.

iOS: E-Mail-Profileinstellungen

iOS: E-Mail-Profileinstellung	Beschreibung
Übermittlungseinstellungen	
Verschieben von Nachrichten zulassen	Diese Einstellung legt fest, ob Benutzer E-Mail-Nachrichten von diesem Konto auf ein anderes vorhandenes E-Mail-Konto auf einem iOS-Gerät verschieben können.
Zulassen, dass letzte Adressen synchronisiert werden	Diese Einstellung legt fest, ob der Benutzer eines iOS-Gerätes zuletzt verwendete Adressen mit anderen Geräten synchronisieren kann.
Nur in Mail verwenden	Diese Einstellung legt fest, ob andere Apps als die Mail-App auf einem iOS-Gerät dieses Konto zum Senden von E-Mail-Nachrichten verwenden können.
S/MIME aktivieren	Diese Einstellung legt fest, ob der Benutzer eines iOS-Gerätes S/MIME-geschützte E-Mail-Nachrichten senden kann.
Signaturanmeldedaten	Diese Einstellung legt fest, wie Geräte die Zertifikate auswählen, die zum Signieren von Nachrichten erforderlich sind. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME aktivieren“ ausgewählt wurde. Mögliche Werte: • Freigegebenes Zertifikat • SCEP • Benutzeranmeldeinformationen

iOS: E-Mail-Profileinstellung	Beschreibung
	Nachdem Sie den gewünschten Profiltyp ausgewählt haben, geben Sie das Profil für ein freigegebenes Zertifikat, das SCEP-Profil oder das Profil für Benutzeranmeldeinformationen an.
Signieren eines freigegebenen Zertifikats	Diese Einstellung legt für ein Client-Zertifikat das Profil für das freigegebene Zertifikat fest, das ein iOS-Gerät verwendet, um E-Mail-Nachrichten zu signieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME aktivieren“ ausgewählt wurde.
Signatur-SCEP	Diese Einstellung legt das SCEP-Profil fest, das Geräte zum Abrufen der Zertifikate verwenden können, die zum Signieren von E-Mail-Nachrichten mit S/MIME erforderlich sind. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME aktivieren“ ausgewählt wurde.
Signieren von Benutzeranmeldeinformationen	Diese Einstellung legt das Profil für Benutzeranmeldeinformationen fest, mit dessen Hilfe Geräte die Client-Zertifikate abrufen können, die zum Signieren von E-Mail-Nachrichten mit S/MIME erforderlich sind. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME aktivieren“ ausgewählt wurde.
Verschlüsselungsanmeldedaten	Diese Einstellung legt fest, wie Geräte die Zertifikate auswählen, die zum Verschlüsseln von Nachrichten erforderlich sind. Mögliche Werte: • Freigegebenes Zertifikat • SCEP • Benutzeranmeldeinformationen Nachdem Sie den Profiltyp ausgewählt haben, wählen Sie das gewünschte Profil für ein freigegebenes Zertifikat, das SCEP-Profil oder das Profil für Benutzeranmeldeinformationen aus. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME aktivieren“ ausgewählt wurde.
Verschlüsselung eines freigegebenen Zertifikats	Diese Einstellung legt für ein Client-Zertifikat das Profil für das freigegebene Zertifikat fest, das ein iOS-Gerät zum Verschlüsseln von E-Mail-Nachrichten verwenden kann. Die Geräte wählen das geeignete Zertifikat für den Empfänger aus, um die Nachrichten mit S/MIME zu verschlüsseln. Diese Einstellung ist nur dann gültig, wenn die Einstellung „S/MIME aktivieren“ ausgewählt wurde.

iOS: E-Mail-Profileinstellung	Beschreibung
Verschlüsselungs-SCEP	Diese Einstellung legt das SCEP-Profil fest, das Geräte zum Abrufen der Zertifikate verwenden können, die zum Verschlüsseln von E-Mail-Nachrichten mit S/MIME erforderlich sind. Diese Einstellung tritt nur dann in Kraft, wenn die Einstellung „S/MIME aktivieren“ ausgewählt ist.
Verschlüsselung von Benutzeranmeldeinformationen	Diese Einstellung legt das Profil für Benutzeranmeldeinformationen fest, mit dessen Hilfe Geräte die Client-Zertifikate abrufen können, die zum Verschlüsseln von E-Mail-Nachrichten mit S/MIME erforderlich sind. Diese Einstellung tritt nur dann in Kraft, wenn die Einstellung „S/MIME aktivieren“ ausgewählt ist.
Nachrichten verschlüsseln	Diese Einstellung legt fest, ob alle Nachrichten vor dem Senden verschlüsselt werden müssen oder ob der Benutzer entscheiden kann, welche Nachrichten er verschlüsselt. Wenn Sie die Einstellung „S/MIME aktivieren“ wählen, müssen standardmäßig alle Nachrichten verschlüsselt werden. Der Standardwert ist „Erforderlich“. Diese Einstellung tritt nur dann in Kraft, wenn die Einstellung „S/MIME aktivieren“ ausgewählt ist. Die Mindestanforderung ist iOS Version 8.0.
Tage für Synchronisierung	Diese Einstellung legt fest, für wie viele Tage in der Vergangenheit E-Mail-Nachrichten und Terminplanerdaten auf ein iOS-Gerät synchronisiert werden sollen. Mögliche Werte: • 1 Tag • 3 Tage • 7 Tage • 14 Tage • 1 Monat • Andauernd Der Standardwert ist „7 Tage“. **Hinweis:** Diese Einstellung betrifft nur die Standard-Mail- und Standard-Terminplaner-App auf iOS-Geräten mit Aktivierungstyp „MDM-Steuerelemente“. Wenn dem Gerät der Aktivierungstyp „Geschäftlich und persönlich – Benutzer-Datenschutz“ oder „Geschäftlich und persönlich – vollständige Kontrolle“ zugewiesen wurde, hat diese Einstellung weder Auswirkungen auf die Synchronisationseinstellungen für die Standard-Mail- und die Standard-Terminplaner-App noch auf die Work Connect-App.

iOS: E-Mail-Profileinstellung	Beschreibung
Authentifizierungstyp	Diese Einstellung legt fest, welche Art der Authentifizierung ein iOS-Gerät verwendet, um eine Verbindung zum Mailserver aufzubauen. Mögliche Werte: • Keine • Freigegebenes Zertifikat • SCEP • Benutzeranmeldeinformationen Der Standardwert ist „Keine“.
Profil für freigegebenes Zertifikat	Diese Einstellung legt für das Client-Zertifikat das Profil für das freigegebene Zertifikat fest, das ein iOS-Gerät verwendet, um eine Verbindung zum Mailserver aufzubauen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Freigegebenes Zertifikat“ gesetzt ist.
Verknüpftes SCEP-Profil	Diese Einstellung legt das verknüpfte SCEP-Profil fest, mit dem der Benutzer eines iOS-Geräts ein Client-Zertifikat für die Authentifizierung beim Mailserver anmeldet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „SCEP“ gesetzt ist.
Verknüpftes Profil für Benutzeranmelde-informationen	Diese Einstellung legt das verknüpfte Profil für Benutzeranmeldeinformationen fest, mit denen der Benutzer eines iOS-Geräts ein Client-Zertifikat für die Authentifizierung beim Mailserver registriert. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Benutzeranmeldeinformationen“ gesetzt ist.
Anmeldedaten und Zertifikat verwenden	Diese Einstellung legt fest, ob ein Gerät die mit dem verknüpften SCEP-Profil erhaltenen Benutzeranmeldeinformationen und ein Client-Zertifikat für die Authentifizierung beim E-Mail-Server verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „SCEP“ gesetzt ist.
SSL verwenden	Diese Einstellung legt fest, ob ein Gerät SSL verwenden muss, um eine Verbindung zum Mailserver aufzubauen.
Alle SSL-Zertifikate akzeptieren	Diese Einstellung legt fest, ob Geräte mit Secure Work Space nicht vertrauenswürdige SSL-Zertifikate vom Mailserver annehmen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „SSL verwenden“ ausgewählt wurde.

iOS: E-Mail-Profileinstellung	Beschreibung
Externe E-Mail-Domänen	
Liste der zulässigen externen E-Mail-Domänen	Diese Einstellung gibt die Liste der Domänen an, an die ein Benutzer E-Mail-Nachrichten oder Kalendereinträge senden kann. Wenn beispielsweise ein Benutzer einen Empfänger, der über eine E-Mail-Adresse in der zugelassenen Domäne verfügt, zu einer E-Mail-Nachricht oder einem Kalendereintrag hinzufügt, wird keine Warnmeldung angezeigt. Diese Einstellung betrifft nur den geschäftlichen Bereich. Wenn Sie hierzu mehrere Domänennamen auflisten, trennen Sie diese durch ein Komma (,), Semikolon (;) oder ein Leerzeichen.
Liste der verbotenen externen E-Mail-Domänen	Diese Einstellung gibt die Liste der Domänen an, an die ein Benutzer keine E-Mail-Nachrichten oder Kalendereinträge senden kann. Wenn beispielsweise ein Benutzer versucht, einen Empfänger, der über eine E-Mail-Adresse in der gesperrten Domäne verfügt, zu einer E-Mail-Nachricht oder einer Kalendereinladung hinzuzufügen, verhindert die Work Connect-App, dass der Benutzer die Aufgabe abschließen kann. Diese Einstellung betrifft nur den geschäftlichen Bereich. Wenn Sie hierzu mehrere Domänennamen auflisten, trennen Sie diese durch ein Komma (,), Semikolon (;) oder ein Leerzeichen.

Android: E-Mail-Profileinstellungen

Android: E-Mail-Profileinstellung	Beschreibung
Übermittlungseinstellungen	
Tage für Synchronisierung	Diese Einstellung legt fest, für wie viele Tage in der Vergangenheit E-Mail-Nachrichten und Terminplanerdaten auf ein Android-Gerät synchronisiert werden sollen. Mögliche Werte: • Unbeschränkt • 1 Tag • 3 Tage • 7 Tage • 14 Tage • 1 Monat Der Standardwert ist „1 Monat“.

Android: E-Mail-Profileinstellung	Beschreibung
	Wenn Sie bei Android-Geräten, die KNOX MDM verwenden, den Wert auf „Unbeschränkt“ setzen, wird nur ein Monat synchronisiert. **Hinweis:** Diese Einstellung betrifft nur die Standard-Mail- und Standard-Terminplaner-App auf Android-Geräten mit Aktivierungstyp „MDM-Steuerelemente“. Wenn dem Gerät der Aktivierungstyp „Geschäftlich und persönlich – Benutzer-Datenschutz“ oder „Geschäftlich und persönlich – vollständige Kontrolle“ zugewiesen wurde, hat diese Einstellung weder Auswirkungen auf die Synchronisationseinstellungen für die Standard-Mail- und die Standard-Terminplaner-App noch auf die Work Space Manager-App.
Authentifizierungstyp	Diese Einstellung legt fest, welche Art der Authentifizierung ein Android-Gerät verwendet, um eine Verbindung zum Mailserver aufzubauen. Mögliche Werte: • Keine • Freigegebenes Zertifikat • SCEP • Benutzeranmeldeinformationen Der Standardwert ist „Keine“.
Verknüpftes SCEP-Profil	Diese Einstellung legt das verknüpfte SCEP-Profil fest, das ein Android-Gerät verwendet, um ein Client-Zertifikat für die Authentifizierung beim E-Mail-Server abzurufen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „SCEP“ gesetzt ist.
Anmeldedaten und Zertifikat verwenden	Diese Einstellung legt fest, ob ein Gerät die mit dem verknüpften SCEP-Profil erhaltenen Benutzeranmeldeinformationen und ein Client-Zertifikat für die Authentifizierung beim E-Mail-Server verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „SCEP“ gesetzt ist.
Profil für freigegebenes Zertifikat	Diese Einstellung legt für das Client-Zertifikat das Profil für das freigegebene Zertifikat fest, das ein Android-Gerät verwendet, um eine Verbindung zum Mailserver aufzubauen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Freigegebenes Zertifikat“ gesetzt ist.
Verknüpftes Profil für Benutzeranmelde-informationen	Diese Einstellung legt das Profil für Benutzeranmeldeinformationen für das Client-Zertifikat fest, mit dem ein Android-Gerät eine Verbindung zum Mailserver aufbaut.

Android: E-Mail-Profileinstellung	Beschreibung
	Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Benutzeranmeldeinformationen“ gesetzt ist.
SSL verwenden	Diese Einstellung legt fest, ob ein Gerät SSL verwenden muss, um eine Verbindung zum Mailserver aufzubauen.
Alle SSL-Zertifikate annehmen	Diese Einstellung legt fest, ob Geräte mit Secure Work Space nicht vertrauenswürdige SSL-Zertifikate vom Mailserver annehmen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „SSL verwenden“ ausgewählt wurde.
S/MIME aktivieren	Diese Einstellung legt fest, ob ein Android-Gerät mit Secure Work Space S/MIME-geschützte E-Mail-Nachrichten senden kann.
Smartcard-Authentifizierung für E-Mail erforderlich	Diese Einstellung legt fest, ob für Samsung KNOX-Geräte zur Authentifizierung beim E-Mail-Server eine Smartcard erforderlich ist.
Externe E-Mail-Domänen	
Liste der zulässigen externen E-Mail-Domänen	Diese Einstellung gibt die Liste der Domänen an, an die ein Benutzer E-Mail-Nachrichten oder Kalendereinträge senden kann. Wenn beispielsweise ein Benutzer einen Empfänger, der über eine E-Mail-Adresse in der zugelassenen Domäne verfügt, zu einer E-Mail-Nachricht oder einem Kalendereintrag hinzufügt, wird keine Warnmeldung angezeigt. Diese Einstellung betrifft nur den geschäftlichen Bereich. Wenn Sie hierzu mehrere Domänennamen auflisten, trennen Sie diese durch ein Komma (,), Semikolon (;) oder ein Leerzeichen.
Liste der verbotenen externen E-Mail-Domänen	Diese Einstellung gibt die Liste der Domänen an, an die ein Benutzer keine E-Mail-Nachrichten oder Kalendereinträge senden kann. Wenn beispielsweise ein Benutzer versucht, einen Empfänger, der über eine E-Mail-Adresse in der gesperrten Domäne verfügt, zu einer E-Mail-Nachricht oder einer Kalendereinladung hinzuzufügen, verhindert die E-Mail- oder Kalender-App, dass der Benutzer die Aufgabe abschließen kann. Diese Einstellung betrifft nur den geschäftlichen Bereich. Wenn Sie hierzu mehrere Domänennamen auflisten, trennen Sie diese durch ein Komma (,), Semikolon (;) oder ein Leerzeichen.

Windows Phone: E-Mail-Profileinstellungen

Windows Phone: E-Mail-Profileinstellung	Beschreibung
Übermittlungseinstellungen	
Profiltyp	Diese Einstellung legt fest, ob das Profil Exchange ActiveSync oder IBM Notes Traveler unterstützen soll.
Kontoname	Diese Einstellung legt den Namen des geschäftlichen E-Mail-Kontos fest, der auf dem Windows Phone-Gerät angezeigt wird. Sie können eine Variable wie etwa „%UserEmailAddress%“ verwenden.
Synchronisierungsintervall	Diese Einstellung legt fest, wie häufig ein Windows Phone-Gerät neue E-Mail-Nachrichten vom Mailserver herunterlädt. Mögliche Werte: • Sobald Elemente empfangen werden • Manuell • Alle 15 Minuten • Alle 30 Minuten • Alle 60 Minuten Der Standardwert ist „Wenn Elemente empfangen werden“.
Tage für Synchronisierung	Diese Einstellung legt fest, für wie viele Tage in der Vergangenheit E-Mail-Nachrichten und Terminplanerdaten auf ein Windows Phone-Gerät synchronisiert werden sollen. Mögliche Werte: • Andauernd • 3 Tage • 7 Tage • 14 Tage • 1 Monat Der Standardwert ist „7 Tage“.
SSL verwenden	Diese Einstellung legt fest, ob ein Windows Phone-Gerät SSL verwenden muss, um eine Verbindung zum Mailserver aufzubauen.
Zu synchronisierender Inhalt	

Windows Phone: E-Mail-Profileinstellung	Beschreibung
E-Mail	Diese Einstellung legt fest, ob ein Windows Phone-Gerät E-Mail-Nachrichten mit dem Mailserver synchronisiert.
Kontakte	Diese Einstellung legt fest, ob ein Windows Phone-Gerät Kontakte mit dem Mailserver synchronisiert.
Kalender	Diese Einstellung legt fest, ob ein Windows Phone-Gerät Kalendereinträge mit dem Mailserver synchronisiert.
Aufgabe	Diese Einstellung legt fest, ob ein Windows Phone-Gerät Aufgabendaten mit dem Mailserver synchronisiert. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Profiltyp“ auf „Exchange ActiveSync“ gesetzt ist.

IMAP/POP3-E-Mail-Profileinstellungen

31

Sie können eine Variable in einem beliebigen Textfeld der Profileinstellungen verwenden, um einen Wert zu referenzieren, statt den tatsächlichen Wert anzugeben. BES12 unterstützt vordefinierte Standardvariablen sowie von Ihnen festgelegte benutzerdefinierte Variablen. IMAP/POP3-E-Mail-Profile werden auf den folgenden Gerätetypen unterstützt:

- iOS
- Android
- Windows Phone

In einigen Fällen wird die erforderliche Mindestversion des Gerätebetriebssystems zur Unterstützung einer Einstellung nicht von BES12 unterstützt. Weitere Informationen zu unterstützten Versionen finden Sie in der Kompatibilitätsmatrix in der Dokumentation zu Installation und Upgrade.

Allgemein: IMAP/POP3-E-Mail-Profileinstellungen

Allgemein: IMAP/POP3-E-Mail-Profileinstellung	Beschreibung
E-Mail-Typ	Diese Einstellung legt den Typ des Mailservers fest. Mögliche Werte: • IMAP • POP3 Der Standardwert ist „IMAP“.
Anzeigename	Diese Einstellung legt den Anzeigenamen des Kontos fest. Wenn das Profil für mehrere Benutzer eingerichtet wird, können Sie die Variable „%UserDisplayName%“ verwenden.
E-Mail-Adresse	Diese Einstellung legt die E-Mail-Adresse des Benutzers fest. Wenn das Profil für mehrere Benutzer gilt, können Sie die %UserEmailAddress%-Variable verwenden.
Einstellungen für eingehende E-Mail-Nachrichten	
Hostname oder IP-Adresse	Diese Einstellung legt den Hostnamen oder die IP-Adresse des E-Mail-Servers für eingehende E-Mail fest.
Port	Diese Einstellung legt den Port fest, der für die Verbindung zum E-Mail-Server für eingehende E-Mail verwendet wird.

Allgemein: IMAP/POP3-E-Mail-Profileinstellung	Beschreibung
Benutzername	Diese Einstellung legt den Benutzernamen des Benutzers fest. Wenn das Profil für mehrere Benutzer gilt, können Sie die %UserName%-Variable verwenden.
SSL für eingehende E-Mail-Nachrichten verwenden	Diese Einstellung legt fest, ob ein iOS-, Android- oder Windows Phone-Gerät SSL verwenden muss, um zum Empfangen von E-Mails eine Verbindung zum Mailserver aufzubauen.
Einstellungen für ausgehende E-Mail-Nachrichten	
Hostname oder IP-Adresse	Diese Einstellung legt den Hostnamen oder die IP-Adresse des E-Mail-Servers für ausgehende E-Mail fest.
Port	Diese Einstellung legt den Port fest, der für die Verbindung zum E-Mail-Server für ausgehende E-Mail verwendet wird.
SSL für ausgehende E-Mail-Nachrichten verwenden	Diese Einstellung legt fest, ob ein iOS-, Android- oder Windows Phone-Gerät SSL verwenden muss, um zum Senden von E-Mail-Nachrichten eine Verbindung zum Mailserver aufzubauen.
Authentifizierung für ausgehende E-Mail-Nachrichten erforderlich	Diese Einstellung legt fest, ob sich ein Gerät zum Senden von E-Mail-Nachrichten beim Server authentifizieren muss.
Die gleichen Anmeldeinformationen als Einstellungen für eingehende E-Mail-Nachrichten verwenden	Diese Einstellung legt fest, ob ein iOS-, Android- oder Windows Phone-Gerät für das Empfangen von E-Mail-Nachrichten dieselben Anmeldeinformationen verwendet wie für das Senden von E-Mail-Nachrichten zur Authentifizierung beim Mailserver. Wenn das Gerät für das Empfangen von E-Mail-Nachrichten nicht dieselben Anmeldeinformationen verwendet wie für das Senden von E-Mail-Nachrichten zur Authentifizierung beim Mailserver, dann geben Sie den vom Gerät verwendeten Benutzernamen und das Kennwort ein. Diese Einstellung ist nur gültig, wenn die Einstellung „Authentifizierung für ausgehende E-Mail-Nachrichten erforderlich“ ausgewählt ist.

iOS: IMAP/POP3-E-Mail-Profileinstellungen

iOS: IMAP/POP3-E-Mail-Profileinstellung	Beschreibung
IMAP-Pfadpräfix	Diese Einstellung legt das Präfix zum IMAP-Pfad fest (falls erforderlich). Kontaktieren Sie ggf. Ihren Internetdienstanbieter, um weitere Informationen zu erhalten.

iOS: IMAP/POP3-E-Mail-Profileinstellung	Beschreibung
	Diese Einstellung ist nur dann gültig, wenn der Wert für die Einstellung „E-Mail-Typ“ auf „IMAP“ gesetzt ist.
Verschieben von Nachrichten zulassen	Diese Einstellung legt fest, ob Benutzer E-Mail-Nachrichten von diesem Konto auf ein anderes E-Mail-Konto auf einem iOS-Gerät verschieben können.
Zulassen, dass letzte Adressen synchronisiert werden	Diese Einstellung legt fest, ob der Benutzer eines iOS-Gerätes zuletzt verwendete Adressen mit anderen Geräten synchronisieren kann.
Nur in Mail verwenden	Diese Einstellung legt fest, ob andere Apps als die Mail-App auf einem iOS-Gerät dieses Konto zum Senden von E-Mail-Nachrichten verwenden können.

Android: IMAP/POP3-E-Mail-Profileinstellungen

Android: IMAP/POP3-E-Mail-Profileinstellung	Beschreibung
IMAP-Pfadpräfix	Diese Einstellung legt das Präfix zum IMAP-Pfad fest (falls erforderlich). Kontaktieren Sie ggf. Ihren Internetdienstanbieter, um weitere Informationen zu erhalten. Diese Einstellung ist nur dann gültig, wenn der Wert für die Einstellung „E-Mail-Typ“ auf „IMAP“ gesetzt ist.
Löschen von E-Mail-Nachrichten vom Server	Diese Einstellung legt fest, wann eine E-Mail vom Mailserver gelöscht wird. Mögliche Werte: • Nie • Wenn aus Posteingang gelöscht Der Standardwert ist „Nie“. Diese Einstellung ist nur dann gültig, wenn der Wert für die Einstellung „E-Mail-Typ“ auf „POP3“ gesetzt ist.

Windows Phone: IMAP/POP3-E-Mail-Profileinstellungen

Windows Phone: IMAP/ POP3-E-Mail-Profileinstellung	Beschreibung
Domäne	Diese Einstellung legt die Domäne des E-Mail-Servers fest.
Synchronisierungsintervall	Diese Einstellung legt fest, wie häufig ein Windows Phone-Gerät neue Inhalte vom Mailserver herunterlädt. Mögliche Werte: • Manuell • 15 Minuten • 30 Minuten • 60 Minuten • 2 Stunden Der Standardwert ist „15 Minuten“.
Ursprüngliche Abrufmenge	Diese Einstellung legt fest, für wie viele Tage in der Vergangenheit E-Mail-Nachrichten und Terminplanerdaten auf ein Windows Phone-Gerät synchronisiert werden sollen. Mögliche Werte: • Alle • 7 Tage • 14 Tage • 30 Tage Der Standardwert ist „7 Tage“.

SCEP-Profileinstellungen

32

Sie können eine Variable in einem beliebigen Textfeld der Profileinstellungen verwenden, um einen Wert zu referenzieren, statt den tatsächlichen Wert anzugeben. BES12 unterstützt vordefinierte Standardvariablen sowie von Ihnen festgelegte benutzerdefinierte Variablen. SCEP-Profile werden auf den folgenden Gerätetypen unterstützt:

- BlackBerry 10
- iOS
- Android Mit Secure Work Space, Samsung KNOX und Android for Work

In einigen Fällen wird die erforderliche Mindestversion des Gerätebetriebssystems zur Unterstützung einer Einstellung nicht von BES12 unterstützt. Weitere Informationen zu unterstützten Versionen finden Sie in der Kompatibilitätsmatrix in der Dokumentation zu Installation und Upgrade.

Allgemein: SCEP-Profileinstellungen

Allgemein: SCEP-Profileinstellung	Beschreibung
URL	Diese Einstellung legt die URL für den SCEP-Dienst fest. Die URL sollte das Protokoll, den FQDN, die Portnummer und den SCEP-Pfad (CGI-Pfad, der in der SCEP-Spezifikation definiert wurde) enthalten. Sie müssen einen Wert für diese Einstellung festlegen, um ein Gerät erfolgreich zu aktivieren. SCEP-HTTPS-URLs werden von iOS-Geräten und BlackBerry 10 OS Version 10.3.0 und höher unterstützt.
Instanzname	Diese Einstellung legt den Namen der Zertifizierungsstelleninstanz fest. Der Wert kann jede beliebige Zeichenkette sein, die der SCEP-Dienst versteht. So könnte der Wert beispielsweise ein Domänenname wie etwa „Beispiel.org“ sein. Wenn eine Zertifizierungsstelle mehrere Zertifizierungsstellenzertifikate aufweist, kann anhand dieses Feldes festgelegt werden, welches dieser Zertifikate verwendet wird.
Zertifizierungsstellen-verbindung	Diese Einstellung gibt an, ob die Zertifizierungsstelle Entrust ist oder eine andere Zertifizierungsstelle. Wenn Sie eine oder mehrere Verbindungen in der Entrust-Software Ihrer Organisation konfiguriert haben, können Sie eine der Verbindungen in der Dropdown-Liste auswählen. Wählen Sie „Generisch“ aus, wenn Sie eine beliebige andere Zertifizierungsstelle verwenden. Wenn Sie eine Entrust-Verbindung auswählen, müssen Sie anschließend das passende digitale ID-Profil auswählen und die erforderlichen Werte angeben. Die verfügbaren digitalen ID-Profile variieren abhängig von der Konfiguration durch den Entrust-Administrator.

Allgemein: SCEP-Profileinstellung	Beschreibung
	Der Standardwert ist „Generisch“.
SCEP-Abfragetyp	Diese Einstellung legt fest, ob das SCEP-Abfragekennwort dynamisch generiert oder als statisches Kennwort bereitgestellt wird. Wenn diese Einstellung auf „Statisch“ gesetzt ist, verwenden alle Geräte das gleiche Abfragekennwort. Wenn diese Einstellung auf „Dynamisch“ gesetzt ist, verwendet jedes Gerät ein eindeutiges Kennwort. Mögliche Werte: • Statisch • Dynamisch Der Standardwert ist „Dynamisch“.
URL der Challenge-Kennwortgenerierung	Diese Einstellung legt die URL fest, die Geräte verwenden, um ein dynamisch generiertes Abfragekennwort vom SCEP-Dienst abzurufen. Die URL sollte das Protokoll, den FQDN, die Portnummer und den SCEP-Pfad (CGI-Pfad, der in der SCEP-Spezifikation definiert wurde) enthalten. Wenn Sie ein dynamisches Abfragekennwort verwenden, müssen Sie einen Wert für diese Einstellung festlegen, um BlackBerry 10-Geräte erfolgreich zu aktivieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „SCEP-Abfragetyp“ auf „Dynamisch“ gesetzt ist.
Authentifizierungstyp	Diese Einstellung legt den Authentifizierungstyp fest, den Geräte verwenden, um eine Verbindung zum SCEP-Dienst aufzubauen und ein Abfragekennwort abzurufen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „SCEP-Abfragetyp“ auf „Dynamisch“ gesetzt ist. Mögliche Werte: • Basis • NTLM Der Standardwert ist „Einfach“.
Domäne	Diese Einstellung legt die Domäne fest, die für die NTLM-Authentifizierung verwendet wird, wenn Geräte eine Verbindung zum SCEP-Dienst aufbauen, um ein Abfragekennwort abzurufen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „NTLM“ gesetzt ist.
Benutzername	Diese Einstellung legt den Benutzernamen fest, der zum Abrufen eines Abfragekennworts vom SCEP-Dienst erforderlich ist.

Allgemein: SCEP-Profileinstellung	Beschreibung
	Diese Einstellung ist nur dann gültig, wenn die Einstellung „SCEP-Abfragetyp“ auf „Dynamisch“ gesetzt ist.
Kennwort	Diese Einstellung legt das Kennwort fest, das erforderlich ist, um das Abfragekennwort vom SCEP-Dienst abzurufen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „SCEP-Abfragetyp“ auf „Dynamisch“ gesetzt ist.
Challenge-Kennwort	Diese Einstellung legt das Abfragekennwort fest, das ein Gerät für die Zertifikatsanmeldung verwendet. Wenn Sie ein statisches Abfragekennwort verwenden, müssen Sie einen Wert für diese Einstellung festlegen, um BlackBerry 10-Geräte erfolgreich zu aktivieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „SCEP-Abfragetyp“ auf „Statisch“ gesetzt ist.

BlackBerry 10: SCEP-Profileinstellungen

BlackBerry 10: SCEP-Profileinstellung	Beschreibung
Standard-Antragsteller und SAN verwenden	Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät den Namen des Antragstellers und den alternativen Antragstellernamen für eine Zertifikatsanforderung generiert. Wenn die Einstellung nicht ausgewählt wird, müssen Sie den Antragsteller und den Namenstyp und -wert des alternativen Antragstellers angeben.
Betreff	Diese Einstellung legt den Betreff für das Zertifikat fest, falls dieser für die SCEP-Konfiguration Ihrer Organisation erforderlich ist. Geben Sie den Betreff in folgendem Format ein: „/CN=<*common_name*>/O=<*domain_name*>“. Wenn das Profil für mehrere Benutzer eingerichtet wird, können Sie die Variable „%UserDistinguisedName%“ oder „%UserPrincipalName%“ verwenden. Diese Einstellung ist nur gültig, wenn „Standard-Antragsteller und SAN verwenden“ nicht ausgewählt ist. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.
SAN	Diese Einstellung gibt den Namenstyp und -wert des alternativen Antragstellers für ein Zertifikat an. Diese Einstellung ist nur gültig, wenn „Standard-Antragsteller und SAN verwenden“ nicht ausgewählt ist.

BlackBerry 10: SCEP-Profileinstellung	Beschreibung
	Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.
SAN-Typ	Diese Einstellung legt ggf. den Alternativnamen des Zertifikatempfängers für das Zertifikat fest. Mögliche Werte: • RFC 822-Name • URI • NT-Prinzipalname • DNS-Name Der Standardwert ist „RFC 822-Name“.
SAN-Wert	Diese Einstellung legt die alternative Darstellung des Antragstellers fest. Der Wert muss eine E-Mail-Adresse, der DNS-Name des Servers der Zertifizierungsstelle, die vollqualifizierte URL des Servers oder ein Prinzipalname sein. Die Einstellung „SAN-Typ“ bestimmt den Typ des geeigneten Werts, der angegeben werden muss. Wenn "RFC 822-Name" festgelegt ist, muss der Wert eine gültige E-Mail-Adresse sein. Wenn "URI" festgelegt ist, muss der Wert eine gültige URL sein, die das Protokoll und den FQDN oder die IP-Adresse enthält. Wenn "NT-Prinzipalname" festgelegt ist, muss der Wert ein gültiger Prinzipalname sein. Wenn "DNS-Name" festgelegt ist, muss der Wert ein gültiger FQDN sein.
Schlüsselalgorithmus	Diese Einstellung legt den Algorithmus fest, den ein BlackBerry 10-Gerät verwendet, um das Client-Schlüsselpaar zu generieren. Sie müssen einen Algorithmus auswählen, der von Ihrer Zertifizierungsstelle unterstützt wird. Mögliche Werte: • Keine • RSA • ECC Der Standardwert ist „RSA“.
RSA-Stärke	Diese Einstellung legt die RSA-Stärke fest, die ein BlackBerry 10-Gerät verwendet, um das Client-Schlüsselpaar zu generieren. Sie müssen eine Schlüsselstärke eingeben, die von Ihrer Zertifizierungsstelle unterstützt wird. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Schlüsselalgorithmus“ auf „RSA“ gesetzt ist.

BlackBerry 10: SCEP-Profileinstellung	Beschreibung
	Mögliche Werte: • 1024 • 2048 • 4096 • 8192 • 16384 Der Standardwert ist „1024“.
ECC-Stärke	Diese Einstellung legt die elliptische Kurve fest, die ein BlackBerry 10-Gerät verwendet, um ein Client-Schlüsselpaar zu generieren. Die elliptische Kurve bestimmt die Stärke des Client-Schlüsselpaars. Sie müssen eine elliptische Kurve auswählen, die von Ihrer Zertifizierungsstelle unterstützt wird. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Schlüsselalgorithmus“ auf „ECC“ gesetzt ist. Mögliche Werte: • sect163k1 • sect283k1 • secp192r1 • secp256r1 • secp384r1 • secp521r1 Der Standardwert ist „secp521r1“.
Verschlüsselungsalgorithmus	Diese Einstellung legt den Verschlüsselungsalgorithmus fest, den ein BlackBerry 10-Gerät für die Zertifikatsanmeldungsanforderung verwendet. Mögliche Werte: • Keine • Triple DES • AES (128 Bit) • AES (196-Bit) • AES (256 Bit) Der Standardwert ist „Triple DES“.

BlackBerry 10: SCEP-Profileinstellung	Beschreibung
Hash-Funktion	Diese Einstellung legt die Hashfunktion fest, die ein BlackBerry 10-Gerät für die Zertifikatsanmeldungsanforderung verwendet. Mögliche Werte: • Keine • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512 Der Standardwert ist „SHA-1“.
Zertifikatfingerabdruck	Diese Einstellung legt den hexadezimal-codierten Hash des Stammzertifikats für die Zertifizierungsstelle fest. Sie können folgende Algorithmen verwenden, um den Fingerabdruck festzulegen: MD5, SHA-1, SHA-224, SHA-256, SHA-384 und SHA-512. Sie müssen einen Wert für diese Einstellung festlegen, um ein BlackBerry 10-Gerät erfolgreich zu aktivieren.
Automatische Erneuerung	Diese Einstellung legt fest, wie viele Tage vor Ablauf eines Zertifikats diese automatische Zertifikatserneuerung erfolgen soll. Mögliche Werte sind 1 bis 999.999.999 Tage. Der Standardwert ist „30“.
Schlüsselnutzung	Diese Einstellung gibt die kryptografischen Vorgänge an, die mithilfe des im Zertifikat enthaltenen öffentlichen Schlüssels ausgeführt werden können. Mögliche Auswahlen: • Digitale Signatur • Nichtabstreitbarkeit • Schlüsselverschlüsselung • Datenverschlüsselung • Schlüsselvereinbarung • Schlüsselzertifikat-Signierung • CRL-Signierung • Nur verschlüsseln • Nur entschlüsseln

BlackBerry 10: SCEP-Profileinstellung	Beschreibung
	Die Standardauswahlen lauten „Digital Signatur“, „Schlüsselverschlüsselung“ und „Schlüsselvereinbarung“. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.
Erweiterte Schlüsselnutzung	Diese Einstellung gibt den Zweck des im Zertifikat enthaltenen Schlüssels an. Mögliche Auswahlen: • Server-Authentifizierung • Client-Authentifizierung • Codesignierung • E-Mail-Schutz • Zeitstempel • OCSP-Signierung • Secure Shell Client • Secure Shell Server Die Standardauswahl lautet „Client-Authentifizierung“. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.

iOS: SCEP-Profileinstellungen

iOS: SCEP-Profileinstellung	Beschreibung
BES12 als Proxy für SCEP-Anforderungen verwenden	Diese Einstellung legt fest, ob alle SCEP-Anforderungen von Geräten per BES12 gesendet werden. Wenn sich die Zertifizierungsstelle hinter Ihrer Firewall befindet, können Sie mithilfe dieser Einstellung Client-Zertifikate auf Geräten anmelden, ohne die Zertifizierungsstelle außerhalb der Firewall sichtbar zu machen.
Betreff	Diese Einstellung legt den Betreff für das Zertifikat fest, falls dieser für die SCEP-Konfiguration Ihrer Organisation erforderlich ist. Geben Sie den Betreff in folgendem Format ein: „/CN=<*common_name*>/O=<*domain_name*>“. Wenn das Profil für mehrere Benutzer eingerichtet wird, können Sie die Variable „%UserDistinguisedName%“ oder „%UserPrincipalName%“ verwenden.
Erneute Versuche	Diese Einstellung legt fest, wie oft der Verbindungsaufbau zum SCEP-Dienst wiederholt wird, wenn der erste Verbindungsversuch fehlgeschlagen ist. Mögliche Werte sind 1 bis 999.

iOS: SCEP-Profileinstellung	Beschreibung
	Der Standardwert ist „3“.
Verzögerung erneuter Versuche	Diese Einstellung legt fest, wie viele Sekunden bis zum nächsten Versuch, eine Verbindung zum SCEP-Dienst aufzubauen, verstreichen sollen. Mögliche Werte sind 1 bis 999. Der Standardwert ist 10 Sekunden.
Schlüsselgröße	Diese Einstellung legt die Schlüsselgröße für das Zertifikat fest. Mögliche Werte: • 1024 • 2048 Der Standardwert ist 1024.
Verwendung als digitale Signatur	Diese Einstellung legt fest, ob das angemeldete Zertifikat für digitale Signaturen verwendet werden kann.
Verwendung für Schlüsselverschlüsselung	Diese Einstellung legt fest, ob das angemeldete Zertifikat zum Verschlüsseln verwendet werden kann.
Fingerabdruck	Diese Einstellung legt den Fingerabdruck für das Anmelden eines SCEP-Zertifikats fest. Wenn Ihre Zertifizierungsstelle mit HTTP anstelle von HTTPS arbeitet, verwenden Geräte den Fingerabdruck, um die Identität der Zertifizierungsstelle beim Anmeldevorgang zu bestätigen.
SAN-Typ	Diese Einstellung legt ggf. den Alternativnamen des Zertifikatempfängers für das Zertifikat fest. Mögliche Werte: • Keine • RFC 822-Name • DNS-Name • Einheitlicher Ressourcenbezeichner Der Standardwert ist „Keine“.
SAN-Wert	Diese Einstellung legt die alternative Darstellung des Zertifikatempfängers fest. Der Wert muss eine E-Mail-Adresse, der DNS-Name des Servers der Zertifizierungsstelle oder die vollqualifizierte URL des Servers sein. Die Einstellung „SAN-Typ“ bestimmt den Typ des geeigneten Werts, der angegeben werden muss. Wenn "RFC 822-Name" festgelegt ist, muss der Wert eine gültige E-Mail-Adresse sein.

iOS: SCEP-Profileinstellung	Beschreibung
	Wenn "URI" festgelegt ist, muss der Wert eine gültige URL sein, die das Protokoll und den FQDN oder die IP-Adresse enthält. Wenn "NT-Prinzipalname" festgelegt ist, muss der Wert ein gültiger Prinzipalname sein. Wenn "DNS-Name" festgelegt ist, muss der Wert ein gültiger FQDN sein.
NT-Prinzipalname	Diese Einstellung legt den NT-Prinzipalnamen für die Zertifikatsgenerierung fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „SAN-Typ“ auf etwas anderes als „Keine“ gesetzt ist.
Automatische Erneuerung	Diese Einstellung legt fest, wie viele Tage vor Ablauf eines Zertifikats diese automatische Zertifikatserneuerung erfolgen soll. Mögliche Werte sind 1 bis 365. Der Standardwert ist 30 Tage.
Verschlüsselungsalgorithmus	Diese Einstellung legt den Verschlüsselungsalgorithmus fest, den ein iOS-Gerät für die Zertifikatsanmeldungsanforderung verwendet. Mögliche Werte: • Keine • Triple DES • AES (128-Bit) • AES (196-Bit) • AES (256-Bit) Der Standardwert ist „Triple DES“.
Hashfunktion	Diese Einstellung legt die Hashfunktion fest, die ein iOS-Gerät für die Zertifikatsanmeldungsanforderung verwendet. Mögliche Werte: • Keine • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512 Der Standardwert ist „SHA-1“.

Android: SCEP-Profileinstellungen

Android-Geräte müssen mit der Aktivierungsart „Geschäftlich und persönlich – vollständige Kontrolle“ oder „Geschäftlich und persönlich – Benutzer-Datenschutz“ aktiviert werden, damit sie SCEP-Profile verwenden können.

Android: SCEP-Profileinstellung	**Beschreibung**
Verschlüsselungsalgorithmus	Diese Einstellung legt den Verschlüsselungsalgorithmus fest, den ein Android-Gerät für die Zertifikatsanmeldungsanforderung verwendet. Mögliche Werte: • Keine • Triple DES • AES (128-Bit) • AES (196-Bit) • AES (256-Bit) Der Standardwert ist „Triple DES“.
Hashfunktion	Diese Einstellung legt die Hashfunktion fest, die ein Android-Gerät für die Zertifikatsanmeldungsanforderung verwendet. Mögliche Werte: • Keine • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512 Der Standardwert ist „SHA-1“.
Fingerabdruck des Zertifikats	Diese Einstellung legt den hexadezimal-codierten Hash des Stammzertifikats für die Zertifizierungsstelle fest. Sie können folgende Algorithmen verwenden, um den Fingerabdruck festzulegen: SHA-1, SHA-224, SHA-256, SHA-384 und SHA-512. Sie müssen einen Wert für diese Einstellung festlegen, damit Geräte, auf denen Android for Work oder Samsung KNOX verwendet wird, aktiviert werden können.
Automatische Erneuerung	Diese Einstellung legt fest, wie viele Tage vor Ablauf eines Zertifikats diese automatische Zertifikatserneuerung erfolgen soll. Mögliche Werte sind 1 bis 365.

Android: SCEP-Profileinstellung	Beschreibung
	Der Standardwert ist „30“.
Android for Work/Samsung KNOX	
Betreff	Diese Einstellung legt den Antragsteller für das Zertifikat fest, falls dieses für die SCEP-Konfiguration Ihres Unternehmens erforderlich ist.
SAN-Typ	Diese Einstellung legt ggf. den Alternativnamen des Zertifikatempfängers für das Zertifikat fest. Mögliche Werte: • RFC 822-Name • Uniform Resource Identifier • NT-Prinzipalname • DNS-Name Der Standardwert ist „RFC 822-Name“.
SAN-Wert	Diese Einstellung legt die alternative Darstellung des Antragstellers fest. Der Wert muss eine E-Mail-Adresse, der DNS-Name des Servers der Zertifizierungsstelle, die vollqualifizierte URL des Servers oder ein Prinzipalname sein. Die Einstellung „SAN-Typ“ bestimmt den Typ des geeigneten Werts, der angegeben werden muss. Wenn "RFC 822-Name" festgelegt ist, muss der Wert eine gültige E-Mail-Adresse sein. Wenn "URI" festgelegt ist, muss der Wert eine gültige URL sein, die das Protokoll und den FQDN oder die IP-Adresse enthält. Wenn "NT-Prinzipalname" festgelegt ist, muss der Wert ein gültiger Prinzipalname sein. Wenn "DNS-Name" festgelegt ist, muss der Wert ein gültiger FQDN sein.
Schlüsselalgorithmus	Diese Einstellung legt den Algorithmus fest, den Geräte, auf denen Android for Work oder Samsung KNOX verwendet wird, zum Generieren des Client-Schlüsselpaars verwenden. Sie müssen einen Algorithmus auswählen, der von Ihrer Zertifizierungsstelle unterstützt wird. Mögliche Werte: • Keine • RSA • ECC Der Standardwert ist „RSA“.

Android: SCEP-Profileinstellung	Beschreibung
RSA-Stärke	Diese Einstellung legt die RSA-Stärke fest, die Geräte, auf denen Android for Work oder Samsung KNOX verwendet wird, zum Generieren des Client-Schlüsselpaars verwenden. Sie müssen eine Schlüsselstärke eingeben, die von Ihrer Zertifizierungsstelle unterstützt wird. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Schlüsselalgorithmus“ auf „RSA“ gesetzt ist. Mögliche Werte: • 1024 • 2048 • 4096 • 8192 • 16384 Der Standardwert ist „1024“.
Schlüsselnutzung	Diese Einstellung gibt die kryptografischen Vorgänge an, die mithilfe des im Zertifikat enthaltenen öffentlichen Schlüssels ausgeführt werden können. Mögliche Auswahlen: • Digitale Signatur • Nichtabstreitbarkeit • Schlüsselverschlüsselung • Datenverschlüsselung • Schlüsselvereinbarung • Schlüsselzertifikat-Signierung • CRL-Signierung • Nur verschlüsseln • Nur entschlüsseln Die Standardauswahlen lauten „Digital Signatur“, „Schlüsselverschlüsselung“ und „Schlüsselvereinbarung“.
Erweiterte Schlüsselnutzung	Diese Einstellung gibt den Zweck des im Zertifikat enthaltenen Schlüssels an. Mögliche Auswahlen: • Server-Authentifizierung

Android: SCEP-Profileinstellung	Beschreibung
	• Client-Authentifizierung • Codesignierung • E-Mail-Schutz • Zeitstempel • OCSP-Signierung • Secure Shell Client • Secure Shell Server Die Standardauswahl lautet „Client-Authentifizierung“.
Secure Work Space.	
BES12 als Proxy für SCEP-Anforderungen verwenden	Diese Einstellung legt fest, ob alle SCEP-Anforderungen von Geräten per BES12 gesendet werden. Wenn sich die Zertifizierungsstelle hinter Ihrer Firewall befindet, können Sie mithilfe dieser Einstellung Client-Zertifikate auf Geräten anmelden, ohne die Zertifizierungsstelle außerhalb der Firewall sichtbar zu machen.
Antragsteller (Secure Work Space)	Diese Einstellung legt den Betreff für das Zertifikat fest, falls dieser für die SCEP-Konfiguration Ihrer Organisation erforderlich ist. Geben Sie den Betreff in folgendem Format ein: „/CN=<*common_name*>/O=<*domain_name*>“. Wenn das Profil für mehrere Benutzer eingerichtet wird, können Sie die Variable „%UserDistinguisedName%“ oder „%UserPrincipalName%“ verwenden.
Wiederholungen	Diese Einstellung legt fest, wie oft der Verbindungsaufbau zum SCEP-Dienst wiederholt wird, wenn der erste Verbindungsversuch fehlgeschlagen ist. Mögliche Werte sind 1 bis 999. Der Standardwert ist „3“.
Wiederholungsverzögerung	Diese Einstellung legt fest, wie viele Sekunden bis zum nächsten Versuch, eine Verbindung zum SCEP-Dienst aufzubauen, verstreichen sollen. Mögliche Werte sind 1 bis 999. Der Standardwert ist 10 Sekunden.
Schlüsselgröße	Diese Einstellung legt die Schlüsselgröße für das Zertifikat fest. Mögliche Werte: • 1024 • 2048

Android: SCEP-Profileinstellung	Beschreibung
	• 4096 • 8192 • 16384 Der Standardwert ist „1024“.
Als digitale Signatur verwenden	Diese Einstellung legt fest, ob das angemeldete Zertifikat für digitale Signaturen verwendet werden kann.
Für Schlüsselverschlüsselung verwenden	Diese Einstellung legt fest, ob das angemeldete Zertifikat zum Verschlüsseln verwendet werden kann.
SAN-Typ	Diese Einstellung legt ggf. den Alternativnamen des Zertifikatempfängers für das Zertifikat fest. Mögliche Werte: • Keine • RFC 822-Name • DNS-Name • Uniform Resource Identifier Der Standardwert ist „Keine“.
SAN-Wert	Diese Einstellung legt die alternative Darstellung des Zertifikatempfängers fest. Der Wert muss eine E-Mail-Adresse, der DNS-Name des Servers der Zertifizierungsstelle oder die vollqualifizierte URL des Servers sein. Die Einstellung „Alternativname Zertifikatempfänger“ betrifft diese Einstellung. Welcher Wert für diese Einstellung geeignet ist, hängt von dem Wert ab, der für die Einstellung „SAN-Typ“ gewählt wurde.
NT-Prinzipalname	Diese Einstellung legt den NT-Prinzipalnamen für die Zertifikatsgenerierung fest. Die Einstellung „Alternativname Zertifikatempfänger“ betrifft diese Einstellung. Welcher Wert für diese Einstellung geeignet ist, hängt von dem Wert ab, der für die Einstellung „SAN-Typ“ gewählt wurde.

Wi-Fi-Profileinstellungen

33

Sie können eine Variable in einem beliebigen Textfeld der Profileinstellungen verwenden, um einen Wert zu referenzieren, statt den tatsächlichen Wert anzugeben. BES12 unterstützt vordefinierte Standardvariablen sowie von Ihnen festgelegte benutzerdefinierte Variablen. Wi-Fi-Profile werden auf den folgenden Gerätetypen unterstützt:

- BlackBerry 10
- iOS
- Android
- Windows Phone

In einigen Fällen wird die erforderliche Mindestversion des Gerätebetriebssystems zur Unterstützung einer Einstellung nicht von BES12 unterstützt. Weitere Informationen zu unterstützten Versionen finden Sie in der Kompatibilitätsmatrix in der Dokumentation zu Installation und Upgrade.

Allgemein: Wi-Fi-Profileinstellungen

Allgemein: Wi-Fi-Profileinstellung	Beschreibung
SSID	Diese Einstellung gibt den Netzwerknamen eines Wi-Fi-Netzwerks und seiner drahtlosen Zugriffspunkte an. Bei der SSID muss die Groß- und Kleinschreibung beachtet werden, und sie muss alphanumerische Zeichen enthalten. Mögliche Werte sind auf 32 Zeichen begrenzt.
Verborgenes Netzwerk	Diese Einstellung legt fest, ob die SSID im Wi-Fi-Netzwerk verborgen ist.

BlackBerry 10: Wi-Fi-Profileinstellungen

BlackBerry 10: Wi-Fi-Profileinstellung	Beschreibung
Sicherheitstyp	Diese Einstellung legt den Sicherheitstyp fest, den das Wi-Fi-Netzwerk verwendet. Mögliche Werte: • Keine • WEP persönlich • WPA-Personal

BlackBerry 10: Wi-Fi-Profileinstellung	Beschreibung
	• WPA - geschäftlich • WPA2-Personal • WPA2 - geschäftlich Der Standardwert ist „Keine“.
WEP-Schlüssel	Diese Einstellung legt den WEP-Schlüssel für das Wi-Fi-Netzwerk fest. Der WEP-Schlüssel muss 10 oder 26 hexadezimale Zeichen (0-9, A-F) oder 5 bzw. 13 alphanumerische Zeichen (0-9, A-Z) umfassen. Beispiele für hexadezimale Schlüsselwerte sind „ABCDEF0123“ oder „ABCDEF0123456789ABCDEF0123“. Beispiele für alphanumerische Schlüsselwerte sind „abCD5“ oder „abCDefGHijKL1“. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP persönlich“ gesetzt ist.
Vorinstallierter Schlüsseltyp	Diese Einstellung legt den Typ des vorinstallierten Schlüssels für das Wi-Fi-Netzwerk fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA-Personal“ oder „WPA2-Personal“ gesetzt ist. Mögliche Werte: • ASCII • HEX Der Standardwert ist „ASCII“.
Preshared key	Diese Einstellung legt den vorinstallierten Schlüssel für das Wi-Fi-Netzwerk fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA-Personal“ oder „WPA2-Personal“ gesetzt ist. Mögliche Werte sind auf 64 Zeichen begrenzt.
Authentifizierungsprotokoll	Diese Einstellung legt die EAP-Methode fest, die das Wi-Fi-Netzwerk verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA - geschäftlich“ oder „WPA2 - geschäftlich“ gesetzt ist. Mögliche Werte: • PEAP • TTLS

BlackBerry 10: Wi-Fi-Profileinstellung	Beschreibung
	• EAP-FAST • TLS Der Standardwert ist „PEAP“.
Interne Authentifizierung	Diese Einstellung legt fest, welche interne Authentifizierungsmethode mit einem TLS-Tunnel verwendet wird. Wenn Sie PAP als interne Authentifizierungsmethode verwenden möchten, setzen Sie diese Einstellung auf „Automatisch“. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „PEAP“ oder „TTLS“ gesetzt ist. Mögliche Werte: • Automatisch • MS-CHAPv2 • GTC Der Standardwert ist „Automatisch“.
EAP-FAST-Provisionierungsmethode	Diese Einstellung legt die Provisionierungsmethode für die EAP-FAST-Authentifizierung fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „EAP-FAST“ gesetzt ist. Mögliche Werte: • Anonym • Authentifiziert Der Standardwert ist „Anonym“.
Benutzername	Diese Einstellung legt den Benutzernamen fest, den ein BlackBerry-Gerät verwendet, um sich beim Wi-Fi-Netzwerk zu authentifizieren. Wenn das Profil für mehrere Benutzer gilt, können Sie die %UserName%-Variable angeben. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „PEAP“, „TTLS“, „EAP-FAST“ oder „TLS“ gesetzt ist.
Kennwort	Diese Einstellung legt das Kennwort fest, das ein BlackBerry-Gerät verwendet, um sich beim Wi-Fi-Netzwerk zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „PEAP“, „TTLS“ oder „EAP-FAST“ gesetzt ist.

BlackBerry 10: Wi-Fi-Profileinstellung	Beschreibung
Bandtyp	Diese Einstellung legt das Frequenzband fest, das vom Wi-Fi-Netzwerk verwendet wird. Mögliche Werte: • Dual • 2,4 GHz • 5,0 GHz Der Standardwert ist „Dual“.
DHCP aktivieren	Diese Einstellung legt fest, ob das Wi-Fi-Netzwerk DHCP verwendet.
IP-Adresse	Diese Einstellung legt die IP-Adresse des Hosts für das Wi-Fi-Netzwerk fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „DHCP aktivieren“ nicht ausgewählt ist.
Subnetzmaske	Diese Einstellung legt die Subnetzmaske in Dezimalschreibweise mit Punkt fest (beispielsweise „192.0.2.0“). Diese Einstellung ist nur dann gültig, wenn die Einstellung „DHCP aktivieren“ nicht ausgewählt ist.
Primärer DNS	Diese Einstellung legt den primären DNS-Server in Dezimalschreibweise mit Punkt fest (beispielsweise „192.0.2.0“). Diese Einstellung ist nur dann gültig, wenn die Einstellung „DHCP aktivieren“ nicht ausgewählt ist.
Sekundärer DNS	Diese Einstellung legt den sekundären DNS-Server in Dezimalschreibweise mit Punkt fest (beispielsweise „192.0.2.0“). Diese Einstellung ist nur dann gültig, wenn die Einstellung „DHCP aktivieren“ nicht ausgewählt ist.
Standard-Gateway	Diese Einstellung legt das Standard-Gateway in Dezimalschreibweise mit Punkt fest (beispielsweise „192.0.2.0“). Diese Einstellung ist nur dann gültig, wenn die Einstellung „DHCP aktivieren“ nicht ausgewählt ist.
Suffix der Domäne	Diese Einstellung legt den FQDN des DNS-Suffixes fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „DHCP aktivieren“ nicht ausgewählt ist.

BlackBerry 10: Wi-Fi-Profileinstellung	Beschreibung
IPv6 aktivieren	Diese Einstellung legt fest, ob das Wi-Fi-Netzwerk IPv6 unterstützt.
Zugriffspunkt-Übergabe aktivieren	Diese Einstellung gibt an, ob ein BlackBerry-Gerät Wi-Fi-Übergaben zwischen drahtlosen Zugriffspunkten ausführen kann.
Benutzerdefinierbar	Dieses Feld gibt die Wi-Fi-Funktionen an, die ein BlackBerry-Gerätebenutzer ändern kann. Wenn diese Einstellung auf „Schreibgeschützt“ gesetzt ist, kann der Benutzer keine Einstellung ändern. Wenn diese Einstellung auf „Nur Anmeldedaten“ gesetzt ist, kann der Benutzer den Benutzernamen und das Kennwort ändern. Mögliche Werte: • Schreibgeschützt • Nur Anmeldedaten Der Standardwert ist „Schreibgeschützt“.
Datensicherheitsebene	Diese Einstellung legt die Domäne im geschäftlichen Bereich fest, in der das Wi-Fi-Profil gespeichert ist, wenn der geschäftliche Bereich mit erweitertem Schutz von Daten im Ruhestand arbeitet. Diese Einstellung ist nur dann gültig, wenn die IT-Richtlinienregel „Erweiterten Schutz von Daten im Ruhestand erzwingen“ ausgewählt ist. Wenn diese Einstellung auf „Immer verfügbar“ gesetzt ist, wird das Profil in der Startdomäne gespeichert und steht zur Verfügung, wenn der geschäftliche Bereich gesperrt ist. Wenn diese Einstellung auf „Verfügbar nach Authentifizierung“ gesetzt ist, wird das Profil in der Betriebsdomäne gespeichert und ist nach dem Entsperren des geschäftlichen Bereichs so lange verfügbar, bis das Gerät erneut gestartet wird. Wenn diese Einstellung auf „Nur verfügbar, wenn der geschäftliche Bereich entsperrt ist“ gesetzt ist, wird das Profil in der Sperrdomäne gespeichert und kann nur dann für Wi-Fi-Verbindungen verwendet werden, wenn der geschäftliche Bereich entsperrt ist. Mögliche Werte: • Immer verfügbar • Verfügbar nach Authentifizierung • Nur verfügbar, wenn der geschäftliche Bereich entsperrt ist Der Standardwert ist „Immer verfügbar“. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.
Vertrauen	
Quelle des Client-Zertifikats	Diese Einstellung legt fest, wie BlackBerry 10-Geräte das Client-Zertifikat abrufen können. Für den Abruf von Client-Zertifikaten über die Geräte stehen vier Möglichkeiten zur Verfügung:

BlackBerry 10: Wi-Fi-Profileinstellung	Beschreibung
	• Wenn Sie „SCEP“ wählen, müssen Sie auch das verknüpfte SCEP-Profil festlegen, das vom Gerät verwendet werden kann, um das Client-Zertifikat herunterzuladen. • Wenn Sie „Benutzeranmeldeinformationen“ wählen, müssen Sie auch das Profil für die Benutzeranmeldeinformationen festlegen, das das Gerät verwenden kann, um das Client-Zertifikat herunterzuladen. • Wenn Sie „Smartcard“ wählen, muss der Benutzer das Gerät mit einer Smartcard pairen, die das Client-Zertifikat enthält. • Wenn Sie „Sonstiges“ wählen, muss der Benutzer das Client-Zertifikat manuell zum Gerät hinzufügen. Smartcard-Unterstützung steht für Geräte zur Verfügung, auf denen BlackBerry 10 OS Version 10.3.1 oder höher ausgeführt wird. Mögliche Werte: • Smartcard • SCEP • Benutzeranmeldeinformationen • Sonstiges Der Standardwert ist „Sonstiges“.
Verknüpftes SCEP-Profil	Diese Einstellung legt das verknüpfte SCEP-Profil fest, mit dem der Benutzer eines BlackBerry 10-Geräts ein Client-Zertifikat für die Authentifizierung beim Wi-Fi-Netzwerk anmeldet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Quelle des Client-Zertifikats“ auf „SCEP“ gesetzt ist.
Verknüpftes Profil für Benutzeranmeldeinformationen	Diese Einstellung legt das verknüpfte Profil für Benutzeranmeldeinformationen fest, das ein BlackBerry 10-Gerät verwendet, um ein Client-Zertifikat für die Authentifizierung beim Wi-Fi-Netzwerk anzumelden. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Quelle des Client-Zertifikats“ auf „Benutzeranmeldeinformationen“ gesetzt ist. Die Mindestanforderung für die Verwendung eines Profils für Benutzeranmeldeinformationen ist BlackBerry 10 OS-Version 10.3.1.
Quelle des vertrauenswürdigen Zertifikats	Diese Einstellung legt die Quelle des vertrauenswürdigen Zertifikats fest. Wenn diese Einstellung auf „Speicher für vertrauenswürdige Zertifikate“ gesetzt ist, kann ein BlackBerry-Gerät eine Verbindung zu einem Wi-Fi-Netzwerk aufbauen, das ein beliebiges Zertifikat im Wi-Fi-Zertifikatspeicher verwendet.

BlackBerry 10: Wi-Fi-Profileinstellung	Beschreibung
	Mögliche Werte: • Keine • Speicher für vertrauenswürdige Zertifikate Der Standardwert ist „Keine“.
Verknüpfte Profile	
Enterprise-Konnektivitäts-Profil mit BlackBerry Secure Connect Plus-Verbindung für geschäftliche Daten verwenden	Diese Einstellung legt fest, ob der gesamte Datenverkehr des geschäftlichen Bereichs über BlackBerry Secure Connect Plus geleitet werden soll, selbst wenn BlackBerry 10-Geräte Zugriff auf das Wi-Fi-Netzwerk haben. Wenn Sie diese Einstellung nicht wählen, wenn Sie ein Wi-Fi-Profil konfigurieren und es BlackBerry 10-Geräten zuweisen, erhält auf den Geräten das geschäftliche Wi-Fi-Netzwerk für den Datenverkehr des geschäftlichen Bereichs Vorrang vor BlackBerry Secure Connect Plus. Wenn Sie diese Funktion verwenden möchten, vergewissern Sie sich, dass in der den Benutzern von BlackBerry 10-Geräten zugewiesenen IT-Richtlinie die IT-Richtlinienregel **Steuerung des Netzwerkzugriffs für geschäftliche Apps erzwingen** nicht ausgewählt ist. Diese Einstellung kann sich auf Datennutzung und Netzwerkkosten in Ihrem Unternehmen auswirken. Vergewissern Sie sich, dass dies die bevorzugte Konfiguration im Unternehmen ist, bevor Sie diese Funktion verwenden. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.2.
Verknüpftes VPN-Profil	Diese Einstellung legt das verknüpfte VPN-Profil fest, das ein BlackBerry-Gerät verwendet, um eine Verbindung zu einem VPN aufzubauen, wenn das Gerät mit dem Wi-Fi-Netzwerk verbunden ist.
Verknüpftes Proxy-Profil	Diese Einstellung legt das verknüpfte Proxy-Profil fest, das ein BlackBerry-Gerät verwendet, um eine Verbindung zu einem Proxy-Server aufzubauen, wenn das Gerät mit dem Wi-Fi-Netzwerk verbunden ist.

iOS: Wi-Fi-Profileinstellungen

iOS: Wi-Fi-Profileinstellung	Beschreibung
Automatisch dem Netzwerk beitreten	Diese Einstellung legt fest, ob ein iOS-Gerät dem Wi-Fi-Netzwerk automatisch beitreten kann.

iOS: Wi-Fi-Profileinstellung	Beschreibung
Verknüpftes Proxy-Profil	Diese Einstellung legt das verknüpfte Proxy-Profil fest, das ein iOS-Gerät verwendet, um eine Verbindung zu einem Proxy-Server aufzubauen, wenn das Gerät mit dem Wi-Fi-Netzwerk verbunden ist.
Netzwerktyp	Diese Einstellung legt eine Konfiguration für das Wi-Fi-Netzwerk fest. Hotspot-Konfigurationen stehen nur für iOS-Geräte zur Verfügung. Um Wi-Fi-Einstellungen für BlackBerry-, Android- und Windows Phone-Geräte zu konfigurieren, müssen Sie ein separates Wi-Fi-Profil erstellen. Mögliche Werte: • Standard • Legacy-Hotspot • Hotspot 2.0 Der Standardwert ist „Standard“.
Angezeigter Betreibername	Diese Einstellung legt den Anzeigenamen des Hotspot-Betreibers fest. Diese Einstellung ist nur dann gültig, wenn der „Netzwerktyp“ auf „Hotspot 2.0“ gesetzt ist.
Domänenname	Diese Einstellung legt den Domänennamen des Hotspot-Betreibers fest. Diese Einstellung ist nur dann gültig, wenn der „Netzwerktyp“ auf „Hotspot 2.0“ gesetzt ist. Wenn Sie diese Einstellung verwenden, ist die Einstellung „SSID“ nicht erforderlich.
Unternehmensbezeichner der Roaming-Konsortien	Diese Einstellung legt die Organisationsbezeichner der Roaming-Konsortien und Dienstanbieter fest, auf die über den Hotspot zugegriffen werden kann. Diese Einstellung ist nur dann gültig, wenn der „Netzwerktyp“ auf „Hotspot 2.0“ gesetzt ist.
NAI-Bereichsnamen	Diese Einstellung legt die NAI-Bereichsnamen fest, die ein iOS-Gerät authentifizieren können. Diese Einstellung ist nur dann gültig, wenn der „Netzwerktyp“ auf „Hotspot 2.0“ gesetzt ist.
MCC/MNCs	Diese Einstellung legt die MCC/MNC-Kombinationen fest, die Mobilfunknetzbetreiber identifizieren. Jeder Wert muss genau sechs Ziffern umfassen. Diese Einstellung ist nur dann gültig, wenn der „Netzwerktyp“ auf „Hotspot 2.0“ gesetzt ist.
Verbindungsaufbau zu Roaming-Partnernetzwerken zulassen	Diese Einstellung legt fest, ob ein iOS-Gerät eine Verbindung zu Roaming-Partnern für den Hotspot aufbauen kann. Diese Einstellung ist nur dann gültig, wenn der „Netzwerktyp“ auf „Hotspot 2.0“ gesetzt ist.
Sicherheitstyp	Diese Einstellung legt den Sicherheitstyp fest, den das Wi-Fi-Netzwerk verwendet.

iOS: Wi-Fi-Profileinstellung	Beschreibung
	Wenn die Einstellung „Netzwerktyp“ auf „Hotspot 2.0“ gesetzt ist, ist diese Einstellung auf „WPA2 - geschäftlich“ gesetzt. Mögliche Werte: • Keine • WEP persönlich • WEP Unternehmen • WPA-Personal • WPA - geschäftlich • WPA2-Personal • WPA2 - geschäftlich Der Standardwert ist „Keine“.
WEP-Schlüssel	Diese Einstellung legt den WEP-Schlüssel für das Wi-Fi-Netzwerk fest. Der WEP-Schlüssel muss 10 oder 26 hexadezimale Zeichen (0-9, A-F) oder 5 bzw. 13 alphanumerische Zeichen (0-9, A-Z) umfassen. Beispiele für hexadezimale Schlüsselwerte sind „ABCDEF0123“ oder „ABCDEF0123456789ABCDEF0123“. Beispiele für alphanumerische Schlüsselwerte sind „abCD5“ oder „abCDefGHijKL1“. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP persönlich“ gesetzt ist.
Preshared key	Diese Einstellung legt den vorinstallierten Schlüssel für das Wi-Fi-Netzwerk fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA-Personal“ oder „WPA2-Personal“ gesetzt ist.
Protokolle	
Authentifizierungsprotokoll	Diese Einstellung legt die EAP-Methoden fest, die das Wi-Fi-Netzwerk unterstützt. Sie können mehrere EAP-Methoden auswählen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP Unternehmen“, „WPA - geschäftlich“ oder „WPA2 - geschäftlich“ gesetzt ist. Mögliche Auswahlen: • TLS • TTLS • LEAP

iOS: Wi-Fi-Profileinstellung	Beschreibung
	• PEAP • EAP-FAST • EAP-SIM
Interne Authentifizierung	Diese Einstellung legt fest, welche interne Authentifizierungsmethode mit TTLS verwendet wird. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „TTLS“ gesetzt ist. Mögliche Werte: • Keine • PAP • CHAP • MS-CHAP • MS-CHAPv2 Der Standardwert ist „MS-CHAPv2“.
PAC verwenden	Diese Einstellung legt fest, ob die EAP-FAST-Methode geschützte Anmeldeinformationen (Protected Access Credential) verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „EAP-FAST“ gesetzt ist.
PAC bereitstellen	Diese Einstellung legt fest, ob die EAP-FAST-Methode die Bereitstellung von geschützten Anmeldeinformationen zulässt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „EAP-FAST“ gesetzt und die Einstellung „PAC verwenden“ ausgewählt ist.
PAC anonym bereitstellen	Diese Einstellung legt fest, ob die EAP-FAST-Methode die anonyme Bereitstellung von geschützten Anmeldeinformationen zulässt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „EAP-FAST“ gesetzt ist und die Einstellungen „PAC verwenden“ und „PAC bereitstellen“ ausgewählt sind.
Authentifizierung	
Externe Identität für TTLS, PEAP und EAP-FAST	Diese Einstellung legt die externe Identität für einen Benutzer fest, die als Klartext gesendet wird. Sie können einen anonymen Benutzernamen festlegen, um die echte Identität des Benutzers zu verbergen (beispielsweise „anonym“). Der verschlüsselte Tunnel wird

iOS: Wi-Fi-Profileinstellung	Beschreibung
	verwendet, um den echten Benutzernamen zur Authentifizierung beim Wi-Fi-Netzwerk zu senden. Wenn die externe Identität den Bereichsnamen enthält, um die Anforderung weiterzuleiten, muss es sich dabei um den tatsächlichen Bereich des Benutzers handeln (beispielsweise „anonym@Beispiel.com“). Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „TTLS“, „PEAP“ oder „EAP-FAST“ gesetzt ist.
Im Wi-Fi-Profil enthaltenes Kennwort verwenden	Diese Einstellung legt fest, ob das Wi-Fi-Profil das Kennwort für die Authentifizierung enthält. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP Unternehmen“, „WPA - geschäftlich“ oder „WPA2 - geschäftlich“ gesetzt ist.
Kennwort	Diese Einstellung legt das Kennwort fest, das ein iOS-Gerät verwendet, um sich beim Wi-Fi-Netzwerk zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Im Wi-Fi-Profil enthaltenes Kennwort verwenden“ ausgewählt wurde.
Benutzername	Diese Einstellung legt den Benutzernamen fest, den ein iOS-Gerät verwendet, um sich beim Wi-Fi-Netzwerk zu authentifizieren. Wenn das Profil für mehrere Benutzer gilt, können Sie die %UserName%-Variable angeben. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP Unternehmen“, „WPA - geschäftlich“ oder „WPA2 - geschäftlich“ gesetzt ist.
Authentifizierungstyp	Diese Einstellung legt fest, welche Art der Authentifizierung ein iOS-Gerät verwendet, um eine Verbindung zum Wi-Fi-Netzwerk aufzubauen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP Unternehmen“, „WPA - geschäftlich“ oder „WPA2 - geschäftlich“ gesetzt ist. Mögliche Werte: • Keine • Freigegebenes Zertifikat • SCEP • Benutzeranmeldeinformationen Der Standardwert ist „Keine“.
Typ der Zertifikatverknüpfung	Diese Einstellung legt den Typ der Zertifikatverknüpfung für das mit dem Wi-Fi-Profil verknüpfte Client-Zertifikat fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Freigegebenes Zertifikat“ gesetzt ist.

iOS: Wi-Fi-Profileinstellung	Beschreibung
	Mögliche Werte: • Einzelne Referenz • Variable Einfügung Der Standardwert ist „Einzelne Referenz“.
Profil für freigegebenes Zertifikat	Diese Einstellung legt das Profil für das freigegebene Zertifikat mit dem Client-Zertifikat fest, das ein iOS-Gerät verwendet, um sich beim Wi-Fi-Netzwerk zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Zertifikatverknüpfung“ auf „Einzelne Referenz“ gesetzt ist.
Name des Client-Zertifikats	Diese Einstellung legt den Namen des Client-Zertifikats fest, das ein iOS-Gerät verwendet, um sich beim Wi-Fi-Netzwerk zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Zertifikatverknüpfung“ auf „Variable Einfügung“ gesetzt ist.
Verknüpftes SCEP-Profil	Diese Einstellung legt das verknüpfte SCEP-Profil fest, das ein iOS-Gerät verwendet, um ein Client-Zertifikat für die Authentifizierung beim Wi-Fi-Netzwerk abzurufen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „SCEP“ gesetzt ist.
Verknüpftes Profil für Benutzeranmelde-informationen	Diese Einstellung legt das verknüpfte Profil für Benutzeranmeldeinformationen fest, das ein iOS-Gerät verwendet, um ein Client-Zertifikat für die Authentifizierung beim Wi-Fi-Netzwerk abzurufen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Benutzeranmeldeinformationen“ gesetzt ist.
Vertrauen	
Vom Authentifizierungsserver erwartete allgemeine Zertifikatnamen	Diese Einstellung legt die allgemeinen Namen im Zertifikat fest, die der Authentifizierungsserver an das Gerät sendet (beispielsweise „*.Beispiel.com“). Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP Unternehmen“, „WPA - geschäftlich“ oder „WPA2 - geschäftlich“ gesetzt ist.
Typ der Zertifikatverknüpfung	Diese Einstellung legt den Typ der Zertifikatverknüpfung für die mit dem Wi-Fi-Profil verknüpften vertrauenswürdigen Zertifikate fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP Unternehmen“, „WPA - geschäftlich“ oder „WPA2 - geschäftlich“ gesetzt ist. Mögliche Werte:

iOS: Wi-Fi-Profileinstellung	Beschreibung
	• Einzelne Referenz • Variable Einfügung Der Standardwert ist „Einzelne Referenz“.
Profile für Zertifizierungsstellen-zertifikate	Diese Einstellung legt die Profile für Zertifizierungsstellenzertifikate mit den vertrauenswürdigen Zertifikaten fest, die ein iOS-Gerät verwendet, damit das Wi-Fi-Netzwerk als vertrauenswürdig gilt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Zertifikatverknüpfung“ auf „Einzelne Referenz“ gesetzt ist.
Vertrauenswürdige Zertifikatnamen	Diese Einstellung legt die Namen der vertrauenswürdigen Zertifikate fest, die ein iOS-Gerät verwendet, damit das Wi-Fi-Netzwerk als vertrauenswürdig gilt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Zertifikatverknüpfung“ auf „Variable Einfügung“ gesetzt ist.
Benutzerentscheidungen vertrauen	Diese Einstellung legt fest, ob ein iOS-Gerät den Benutzer auffordert, einem Server zu vertrauen, wenn die Vertrauenskette nicht hergestellt werden kann. Wenn diese Einstellung nicht ausgewählt ist, können nur Verbindungen zu von Ihnen festgelegten vertrauenswürdigen Servern aufgebaut werden. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP Unternehmen“, „WPA - geschäftlich“ oder „WPA2 - geschäftlich“ gesetzt ist.

Android: Wi-Fi-Profileinstellungen

Android: Wi-Fi-Profileinstellung	Beschreibung
Verknüpftes Proxy-Profil	Diese Einstellung legt das verknüpfte Proxy-Profil fest, das ein Android for Work-Gerät verwendet, um eine Verbindung zu einem Proxy-Server aufzubauen, wenn das Gerät mit dem Wi-Fi-Netzwerk verbunden ist.
BSSID	Diese Einstellung legt die MAC-Adresse eines drahtlosen Zugriffspunkts im Wi-Fi-Netzwerk fest.
Primärer DNS	Diese Einstellung legt den primären DNS-Server in Dezimalschreibweise mit Punkt fest (beispielsweise „192.0.2.0“). Diese Einstellung gilt nur für Geräte, die Samsung KNOX verwenden, wenn die IP-Adresse über das Unternehmensnetzwerk statisch zugewiesen wird.

Android: Wi-Fi-Profileinstellung	Beschreibung
Sekundärer DNS	Diese Einstellung legt den sekundären DNS-Server in Dezimalschreibweise mit Punkt fest (beispielsweise „192.0.2.0“). Diese Einstellung gilt nur für Geräte, die Samsung KNOX verwenden, wenn die IP-Adresse über das Unternehmensnetzwerk statisch zugewiesen wird.
Sicherheitstyp	Diese Einstellung legt den Sicherheitstyp fest, den das Wi-Fi-Netzwerk verwendet. Mögliche Werte: • Keine • Persönlich • Unternehmen Der Standardwert ist „Keine“.
Persönlicher Sicherheitstyp	Diese Einstellung legt den persönlichen Sicherheitstyp fest, den das Wi-Fi-Netzwerk verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „Persönlich“ gesetzt ist. Mögliche Werte: • Keine • WEP persönlich • WPA-Personal/WPA2-Personal Der Standardwert ist „Keine“.
WEP-Schlüssel	Diese Einstellung legt den WEP-Schlüssel für das Wi-Fi-Netzwerk fest. Der WEP-Schlüssel muss 10 oder 26 hexadezimale Zeichen (0-9, A-F) oder 5 bzw. 13 alphanumerische Zeichen (0-9, A-Z) umfassen. Beispiele für hexadezimale Schlüsselwerte sind „ABCDEF0123“ oder „ABCDEF0123456789ABCDEF0123“. Beispiele für alphanumerische Schlüsselwerte sind „abCD5“ oder „abCDefGHijKL1“. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Persönlicher Sicherheitstyp“ auf „WEP persönlich“ gesetzt ist.
Preshared key	Diese Einstellung legt den vorinstallierten Schlüssel für das Wi-Fi-Netzwerk fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Persönlicher Sicherheitstyp“ auf „WPA-Personal/WPA2-Personal“ gesetzt ist.

Android: Wi-Fi-Profileinstellung	Beschreibung
Authentifizierungsprotokoll	Diese Einstellung legt die EAP-Methode fest, die das Wi-Fi-Netzwerk verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „Unternehmen“ gesetzt ist. Mögliche Werte: • TLS • TTLS • PEAP • LEAP* Der Standardwert ist „TLS“. * Das Authentifizierungsprotokoll wird von Geräten, die Samsung KNOX verwenden, nicht unterstützt.
Interne Authentifizierung	Diese Einstellung legt fest, welche interne Authentifizierungsmethode mit TTLS verwendet wird. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „TTLS“ gesetzt ist. Mögliche Werte: • Keine • PAP • CHAP* • MS-CHAP • MS-CHAPv2 • GTC Der Standardwert ist „MS-CHAPv2“. * Die interne Authentifizierungsmethode wird von Geräten, die Samsung KNOX verwenden, nicht unterstützt.
Externe Identität für TTLS	Diese Einstellung legt die externe Identität für einen Benutzer fest, die als Klartext gesendet wird. Sie können einen anonymen Benutzernamen festlegen, um die echte Identität des Benutzers zu verbergen (beispielsweise „anonym“). Der verschlüsselte Tunnel wird verwendet, um den echten Benutzernamen zur Authentifizierung beim Wi-Fi-Netzwerk zu senden. Wenn die externe Identität den Bereichsnamen enthält, um die Anforderung weiterzuleiten, muss es sich dabei um den tatsächlichen Bereich des Benutzers handeln (beispielsweise „anonym@Beispiel.com“).

Android: Wi-Fi-Profileinstellung	Beschreibung
	Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „TTLS“ gesetzt ist.
Externe Identität für PEAP	Diese Einstellung legt die externe Identität für einen Benutzer fest, die als Klartext gesendet wird. Sie können einen anonymen Benutzernamen festlegen, um die echte Identität des Benutzers zu verbergen (beispielsweise „anonym“). Der verschlüsselte Tunnel wird verwendet, um den echten Benutzernamen zur Authentifizierung beim Wi-Fi-Netzwerk zu senden. Wenn die externe Identität den Bereichsnamen enthält, um die Anforderung weiterzuleiten, muss es sich dabei um den tatsächlichen Bereich des Benutzers handeln (beispielsweise „anonym@Beispiel.com“). Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „PEAP“ gesetzt ist.
Benutzername	Diese Einstellung legt den Benutzernamen fest, den ein Android-Gerät verwendet, um sich beim Wi-Fi-Netzwerk zu authentifizieren. Wenn das Profil für mehrere Benutzer gilt, können Sie die %UserName%-Variable angeben. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „Unternehmen“ gesetzt ist.
Im Wi-Fi-Profil enthaltenes Kennwort verwenden	Diese Einstellung legt fest, ob das Wi-Fi-Profil das Kennwort für die Authentifizierung enthält. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „Unternehmen“ gesetzt ist.
Kennwort	Diese Einstellung legt das Kennwort fest, das ein Android-Gerät verwendet, um sich beim Wi-Fi-Netzwerk zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Im Wi-Fi-Profil enthaltenes Kennwort verwenden“ ausgewählt wurde.
Authentifizierungstyp	Diese Einstellung legt fest, welche Art der Authentifizierung ein Android-Gerät verwendet, um eine Verbindung zum Wi-Fi-Netzwerk aufzubauen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „Unternehmen“ gesetzt ist. Mögliche Werte: • Keine • Freigegebenes Zertifikat • SCEP • Benutzeranmeldeinformationen

Android: Wi-Fi-Profileinstellung	Beschreibung
	Der Standardwert ist „Keine“.
Typ der Zertifikatverknüpfung	Diese Einstellung legt den Typ der Zertifikatverknüpfung für das mit dem Wi-Fi-Profil verknüpfte Client-Zertifikat fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Freigegebenes Zertifikat“ gesetzt ist. Mögliche Werte: • Einzelne Referenz • Variable Einfügung Der Standardwert ist „Einzelne Referenz“.
Profil für freigegebenes Zertifikat	Diese Einstellung legt das Profil für das freigegebene Zertifikat mit dem Client-Zertifikat fest, das ein Android-Gerät verwendet, um sich beim Wi-Fi-Netzwerk zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Zertifikatverknüpfung“ auf „Einzelne Referenz“ gesetzt ist. Der Name des Profils für das freigegebene Zertifikat muss für Geräte, die einen KNOX Workspace verwenden, weniger als 36 Zeichen enthalten.
Verknüpftes SCEP-Profil	Diese Einstellung legt das verknüpfte SCEP-Profil fest, das ein Android-Gerät verwendet, um ein Client-Zertifikat für die Authentifizierung beim Wi-Fi-Netzwerk abzurufen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „SCEP“ gesetzt ist. Der Name des SCEP-Profils muss für Geräte, die einen KNOX Workspace verwenden, weniger als 36 Zeichen enthalten.
Verknüpftes Profil für Benutzeranmeldeinformationen	Diese Einstellung legt das verknüpfte Profil für Benutzeranmeldeinformationen fest, das ein Android-Gerät verwendet, um ein Client-Zertifikat für die Authentifizierung beim Wi-Fi-Netzwerk abzurufen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Benutzeranmeldeinformationen“ gesetzt ist. Der Name des Profils für Benutzeranmeldeinformationen muss für Geräte, die einen KNOX Workspace verwenden, weniger als 36 Zeichen enthalten.
Name des Client-Zertifikats	Diese Einstellung legt den Namen des Client-Zertifikats fest, das ein Android-Gerät verwendet, um sich beim Wi-Fi-Netzwerk zu authentifizieren.

Android: Wi-Fi-Profileinstellung	Beschreibung
	Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Zertifikatverknüpfung“ auf „Variable Einfügung“ gesetzt ist.
Vom Authentifizierungsserver erwartete allgemeine Zertifikatnamen	Diese Einstellung legt die allgemeinen Namen im Zertifikat fest, die der Authentifizierungsserver an das Gerät sendet (beispielsweise „*.Beispiel.com“). Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „Unternehmen“ gesetzt ist.
Typ der Zertifikatverknüpfung	Diese Einstellung legt den Typ der Zertifikatverknüpfung für die mit dem Wi-Fi-Profil verknüpften vertrauenswürdigen Zertifikate fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „Unternehmen“ gesetzt ist. Mögliche Werte: • Einzelne Referenz • Variable Einfügung Der Standardwert ist „Einzelne Referenz“.
Zertifizierungsstellenzertifikat-Profil	Diese Einstellung legt das Profil mit Zertifizierungsstellenzertifikat mit dem vertrauenswürdigen Zertifikat fest, die ein Android-Gerät verwendet, damit das Wi-Fi-Netzwerk als vertrauenswürdig gilt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Zertifikatverknüpfung“ auf „Einzelne Referenz“ gesetzt ist.
Vertrauenswürdige Zertifikatnamen	Diese Einstellung legt die Namen der vertrauenswürdigen Zertifikate fest, die ein Android-Gerät verwendet, damit das Wi-Fi-Netzwerk als vertrauenswürdig gilt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Zertifikatverknüpfung“ auf „Variable Einfügung“ gesetzt ist.

Windows Phone: Wi-Fi-Profileinstellungen

Windows Phone: Wi-Fi-Profileinstellung	Beschreibung
Sicherheitstyp	Diese Einstellung legt den Sicherheitstyp fest, den das Wi-Fi-Netzwerk verwendet. Mögliche Werte:

Windows Phone: Wi-Fi-Profileinstellung	Beschreibung
	• Öffnen • WPA - geschäftlich • WPA-Personal • WPA2 - geschäftlich • WPA2-Personal Der Standardwert ist „Offen“.
Verschlüsselungstyp	Diese Einstellung legt die Verschlüsselungsmethode fest, die das Wi-Fi-Netzwerk verwendet. Die Einstellung „Sicherheitstyp“ legt fest, welche Authentifizierungstypen unterstützt werden und welcher Standardwert für diese Einstellung verwendet wird. Mögliche Werte: • Keine • WEP • TKIP • AES
WEP-Schlüssel	Diese Einstellung legt den WEP-Schlüssel für das Wi-Fi-Netzwerk fest. Der WEP-Schlüssel muss 10 oder 26 hexadezimale Zeichen (0-9, A-F) oder 5 bzw. 13 alphanumerische Zeichen (0-9, A-Z) umfassen. Beispiele für hexadezimale Schlüsselwerte sind „ABCDEF0123“ oder „ABCDEF0123456789ABCDEF0123“. Beispiele für alphanumerische Schlüsselwerte sind „abCD5“ oder „abCDefGHijKL1“. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verschlüsselungstyp“ auf „Offen“ oder „WPA-Personal“ gesetzt ist.
Preshared key	Diese Einstellung legt den vorinstallierten Schlüssel für das Wi-Fi-Netzwerk fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA-Personal“ oder „WPA2-Personal“ gesetzt ist oder die Einstellung „Sicherheitstyp“ auf „Offen“ und die Einstellung „Verschlüsselungstyp“ auf „WEP“ gesetzt ist.
Schlüsselindex	Diese Einstellung legt die Position des entsprechenden, auf dem drahtlosen Zugriffspunkt gespeicherten Schlüssels fest. Mögliche Werte sind 1 bis 4. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „Offen“ und der „Verschlüsselungstyp“ auf „WEP“ gesetzt ist.

Windows Phone: Wi-Fi-Profileinstellung	Beschreibung
Single Sign-On aktivieren	Diese Einstellung legt fest, ob das Wi-Fi-Netzwerk die Authentifizierung nach einmaliger Anmeldung unterstützt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA - geschäftlich“ oder „WPA2 - geschäftlich“ gesetzt ist.
Typ der einmaligen Anmeldung	Diese Einstellung legt fest, wann die Authentifizierung nach einmaliger Anmeldung durchgeführt wird. Wenn diese Einstellung auf „Direkt vor Benutzeranmeldung durchführen“ gesetzt ist, wird die einmalige Anmeldung durchgeführt, bevor sich der Benutzer beim Active Directory Ihrer Organisation anmeldet. Wenn diese Einstellung auf „Direkt nach Benutzeranmeldung durchführen“ gesetzt ist, wird die einmalige Anmeldung sofort durchgeführt, nachdem sich der Benutzer beim Active Directory Ihrer Organisation angemeldet hat. Diese Einstellung ist nur dann gültig, wenn „Einmalige Anmeldung aktivieren“ ausgewählt wurde. Mögliche Werte: • Direkt vor Benutzeranmeldung durchführen • Direkt nach Benutzeranmeldung durchführen Der Standardwert ist „Direkt vor Benutzeranmeldung durchführen“.
Maximale Verzögerung für Konnektivität	Diese Einstellung legt fest, wie viele Sekunden verstreichen sollen, bevor der Versuch, die Verbindung durch eine einmalige Anmeldung aufzubauen, fehlschlägt. Diese Einstellung ist nur dann gültig, wenn „Einmalige Anmeldung aktivieren“ ausgewählt wurde. Mögliche Werte sind 0 bis 120 Sekunden. Der Standardwert ist „10“.
Zulassen, dass weitere Dialoge während der einmaligen Anmeldung angezeigt werden.	Diese Einstellung legt fest, ob ein Gerät außer dem Anmeldebildschirm Dialogfelder anzeigen kann. Wenn es beispielsweise für einen EAP-Authentifizierungstyp erforderlich ist, dass der Benutzer das im Authentifizierungsvorgang vom Server gesendete Zertifikat bestätigt, kann das Gerät das entsprechende Dialogfeld anzeigen. Diese Einstellung ist nur dann gültig, wenn „Einmalige Anmeldung aktivieren“ ausgewählt wurde.
Dieses Netzwerk verwendet separate virtuelle LANs für Geräte- und Benutzerauthentifizierung	Diese Einstellung legt fest, ob von den Anmeldeinformationen des Benutzers abhängt, welches VLAN von einem Gerät verwendet wird. Wenn das Gerät beispielsweise beim Starten in ein VLAN platziert wird und dann – basierend auf Berechtigungen – nach der Anmeldung des Benutzers in ein anderes VLAN-Netzwerk übergeht.

Windows Phone: Wi-Fi-Profileinstellung	Beschreibung
	Diese Einstellung ist nur dann gültig, wenn „Einmalige Anmeldung aktivieren“ ausgewählt wurde.
Serverzertifikat bewerten	Diese Einstellung legt fest, ob ein Gerät das Serverzertifikat bewerten muss, das die Identität des drahtlosen Zugriffspunkts überprüft. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA - geschäftlich“ oder „WPA2 - geschäftlich“ gesetzt ist.
Benutzer nicht auffordern, neue Server oder vertrauenswürdige Zertifizierungsstellen zu autorisieren	Diese Einstellung legt fest, ob ein Benutzer aufgefordert wird, dem Serverzertifikat zu vertrauen. Diese Einstellung ist nur dann gültig, wenn „Serverzertifikat bewerten“ ausgewählt wurde.
Profile für Zertifizierungsstellen-zertifikate	Diese Einstellung legt das Profil des Zertifizierungsstellenzertifikats fest, das den Vertrauensstamm für das vom drahtlosen Zugriffspunkt verwendete Serverzertifikat bereitstellt. Diese Einstellung begrenzt die Stammzertifizierungsstellen, denen Geräte vertrauen, auf die ausgewählten Zertifizierungsstellen. Wenn Sie keine vertrauenswürdigen Stammzertifizierungsstellen auswählen, vertrauen die Geräte allen Stammzertifizierungsstellen, die in ihrem Speicher für vertrauenswürdige Stammzertifizierungsstellen aufgelistet sind. Diese Einstellung ist nur dann gültig, wenn „Serverzertifikat bewerten“ ausgewählt wurde.
Schnelle Wiederherstellung der Verbindung aktivieren	Diese Einstellung legt fest, ob das Wi-Fi-Netzwerk die schnelle Wiederherstellung bei PEAP-Authentifizierung über mehrere drahtlose Zugriffspunkte unterstützt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA - geschäftlich“ oder „WPA2 - geschäftlich“ gesetzt ist.
NAP erzwingen	Diese Einstellung legt fest, ob das Wi-Fi-Netzwerk anhand von NAP Systemintegritätsprüfungen auf Geräten durchführen soll, um zu überprüfen, ob die Geräte den Integritätsanforderungen entsprechen, bevor der Verbindungsaufbau zum Netzwerk zugelassen wird. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA - geschäftlich“ oder „WPA2 - geschäftlich“ gesetzt ist.
PMK-Zwischenspeicherung aktivieren	Diese Einstellung legt fest, ob ein Gerät den PMK zwischenspeichern kann, um ein schnelles WPA2 Roaming einzuschalten. Ein schnelles Roaming überspringt 802.1X-Einstellungen mit einem drahtlosen Zugriffspunkt, bei dem sich das Gerät zuvor authentifiziert hat.

Windows Phone: Wi-Fi-Profileinstellung	Beschreibung
	Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA2-Enterprise“ gesetzt ist.
PMK-Lebenszeit	Diese Einstellung legt fest, wie viele Minuten ein Gerät den PMK im Cache speichern kann. Diese Einstellung ist nur dann gültig, wenn „PMK-Zwischenspeicherung aktivieren“ ausgewählt ist. Mögliche Werte sind 5 bis 1440. Der Standardwert ist „720“.
Anzahl der Einträge im PMK-Cache	Diese Einstellung legt die maximale Anzahl an PMK-Einträgen fest, die ein Gerät im Cache speichern kann. Diese Einstellung ist nur dann gültig, wenn „PMK-Zwischenspeicherung aktivieren“ ausgewählt ist. Mögliche Werte sind 1 bis 255. Der Standardwert ist „128“.
Dieses Netzwerk arbeitet mit Vorauthentifizierung	Diese Einstellung legt fest, ob der Zugriffspunkt die Vorauthentifizierung für ein schnelles WPA2 Roaming unterstützt. Vorauthentifizierung ermöglicht Geräten, die eine Verbindung zu einem drahtlosen Zugriffspunkt aufbauen, 802.1X-Einstellungen mit anderen drahtlosen Zugriffspunkten innerhalb seines Bereichs durchzuführen. Bei einer Vorauthentifizierung werden der PMK und die mit ihm verknüpften Informationen im PMK-Cache gespeichert. Wenn das Gerät eine Verbindung zu einem drahtlosen Zugriffspunkt aufbaut, bei dem es sich vorauthentifiziert hat, verwendet es die zwischengespeicherten PMK-Daten, um die Zeit für die Authentifizierung und den Verbindungsaufbau zu verkürzen. Diese Einstellung ist nur dann gültig, wenn „PMK-Zwischenspeicherung aktivieren“ ausgewählt ist.
Maximale Vorauthentifizierung	Diese Einstellung legt die maximale Anzahl zulässiger Vorauthentifizierungsversuche fest. Diese Einstellung ist nur dann gültig, wenn „Dieses Netzwerk arbeitet mit Vorauthentifizierung“ ausgewählt ist. Mögliche Werte sind 1 bis 16. Der Standardwert ist „3“.

VPN-Profileinstellungen

34

Sie können eine Variable in einem beliebigen Textfeld der Profileinstellungen verwenden, um einen Wert zu referenzieren, statt den tatsächlichen Wert anzugeben. BES12 unterstützt vordefinierte Standardvariablen sowie von Ihnen festgelegte benutzerdefinierte Variablen. VPN-Profile werden auf den folgenden Gerätetypen unterstützt:

- BlackBerry 10
- iOS
- KNOX Workspace

In einigen Fällen wird die erforderliche Mindestversion des Gerätebetriebssystems zur Unterstützung einer Einstellung nicht von BES12 unterstützt. Weitere Informationen zu unterstützten Versionen finden Sie in der Kompatibilitätsmatrix in der Dokumentation zu Installation und Upgrade.

BlackBerry 10: VPN-Profileinstellungen

BlackBerry 10: VPN-Profileinstellung	Beschreibung
Serveradresse	Diese Einstellung legt den FQDN oder die IP-Adresse eines VPN-Servers fest.
Gateway-Typ	Diese Einstellung gibt den Typ des VPN-Client an, den der VPN-Client auf einem BlackBerry 10-Gerät emuliert. Mögliche Werte: • Check Point VPN-1 • Cisco VPN 3000 Series Concentrator • Cisco Secure PIX Firewall • Cisco IOS Easy VPN • Cisco ASA Series • Cisco AnyConnect • Juniper SRX Series (IPsec VPN) • Juniper MAG Series oder Juniper SA Series (SSL VPN) • Microsoft IKEv2 VPN-Server • Generischer IKEv2 VPN-Server Der Standardwert ist „Check Point VPN-1“.
Authentifizierungstyp	Diese Einstellung legt den Authentifizierungstyp für das VPN-Gateway fest.

BlackBerry 10: VPN-Profileinstellung	Beschreibung
	Die Einstellung „Gatewaytyp“ legt fest, welche Authentifizierungstypen unterstützt werden und welcher Standardwert für diese Einstellung verwendet wird. Mögliche Werte: • PSK • PKI • XAUTH-PSK • XAUTH-PKI • EAP-TLS • EAP-MS-CHAPv2
Vorinstallierter Schlüssel oder Gruppenkennwort	Diese Einstellung legt den vorinstallierten Schlüssel oder das Gruppenkennwort für das VPN-Gateway fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „PSK“ oder „XAUTH-PSK“ gesetzt ist.
Benutzername	Diese Einstellung legt den Benutzernamen fest, den ein BlackBerry 10-Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren. Wenn das Profil für mehrere Benutzer gilt, können Sie die %UserName%-Variable verwenden. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Cisco AnyConnect“ oder die Einstellung „Authentifizierungstyp“ auf „XAUTH-PSK“ oder „XAUTH-PKI“ gesetzt ist.
Hardware-Token	Diese Einstellung legt fest, ob ein Benutzer ein Hardware-Token verwenden muss, um sich beim VPN-Gateway zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „XAUTH-PSK“ oder „XAUTH-PKI“ gesetzt ist.
Kennwort	Diese Einstellung legt das Kennwort fest, den ein BlackBerry 10-Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Cisco AnyConnect“ oder die Einstellung „Authentifizierungstyp“ auf „XAUTH-PSK“ oder „XAUTH-PKI“ gesetzt und die Einstellung „Hardware-Token“ nicht ausgewählt ist.
EAP-Identität	Diese Einstellung legt die EAP-Identität fest, die ein BlackBerry 10-Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „EAP-TLS“ gesetzt ist.

BlackBerry 10: VPN-Profileinstellung	Beschreibung
MS-CHAPv2 EAP-Identität	Diese Einstellung legt die MS-CHAPv2 EAP-Identität fest, die ein BlackBerry 10-Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „EAP-MS-CHAPv2“ gesetzt ist.
MS-CHAPv2-Benutzername	Diese Einstellung legt den MS-CHAPv2-Benutzernamen fest, den ein BlackBerry 10-Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „EAP-MS-CHAPv2“ gesetzt ist.
MS-CHAPv2-Kennwort	Diese Einstellung legt das MS-CHAPv2-Kennwort fest, das ein BlackBerry 10-Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „EAP-MS-CHAPv2“ gesetzt ist.
Typ der Authentifizierungs-ID	Diese Einstellung legt den Authentifizierungs-ID-Typ für das VPN-Gateway fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Juniper MAG Series oder Juniper SA Series (SSL VPN)“, „Microsoft IKEv2 VPN-Server“ oder „Generischer IKEv2 VPN-Server“ gesetzt ist. Die Einstellung „Gatewaytyp“ legt fest, welche Authentifizierungs-ID-Typen unterstützt werden und welcher Standardwert für diese Einstellung verwendet wird. Mögliche Werte: • IPv4 • Vollständig qualifizierter Domänenname • E-Mail-Adresse • Distinguished Name des Identitätszertifikats • General Name des Identitätszertifikats
Authentifizierungs-ID oder Gruppenbenutzername	Diese Einstellung legt die Authentifizierungs-ID oder den Gruppenbenutzernamen für das VPN-Gateway fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Juniper MAG Series oder Juniper SA Series (SSL VPN)“, „Microsoft IKEv2 VPN-Server“ oder „Generischer IKEv2 VPN-Server“ gesetzt ist oder wenn die Einstellung „Authentifizierungstyp“ auf „PSK“ oder „XAUTH-PSK“ gesetzt ist.
Gateway-Authentifizierungstyp	Diese Einstellung legt den Gateway-Authentifizierungstyp für das VPN-Gateway fest.

BlackBerry 10: VPN-Profileinstellung	Beschreibung
	Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Juniper MAG Series oder Juniper SA Series (SSL VPN)“, „Microsoft IKEv2 VPN-Server“ oder „Generischer IKEv2 VPN-Server“ gesetzt ist. Mögliche Werte: • Keine • PSK • PKI Der Standardwert ist „Keine“.
Vorinstallierter Gateway-Schlüssel	Diese Einstellung legt den vorinstallierten Gateway-Schlüssel für das VPN-Gateway fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gateway-Authentifizierungstyp“ auf „PSK“ gesetzt ist.
Typ der Gateway-Authentifizierungs-ID	Diese Einstellung legt den Gateway-Authentifizierungs-ID-Typ für das VPN-Gateway fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Juniper MAG Series oder Juniper SA Series (SSL VPN)“, „Microsoft IKEv2 VPN-Server“ oder „Generischer IKEv2 VPN-Server“ gesetzt ist. Mögliche Werte: • IPv4 • Vollständig qualifizierter Domänenname • E-Mail-Adresse • Distinguished Name des Identitätszertifikats • General Name des Identitätszertifikats Der Standardwert ist „IPv4“.
Gateway-Authentifizierungs-ID	Diese Einstellung legt die Gateway-Authentifizierungs-ID für das VPN-Gateway fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gateway-Authentifizierungs-ID“ auf „Vollständig qualifizierter Domänenname“ oder „E-Mail-Adresse“ gesetzt ist.
Sekundärer Benutzername	Diese Einstellung legt den Benutzernamen fest, den ein BlackBerry 10-Gerät für die Sekundär-Authentifizierung beim VPN-Gateway verwendet. Wenn das Profil für mehrere Benutzer gilt, können Sie die %UserName%-Variable verwenden. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Cisco AnyConnect" gesetzt ist.

BlackBerry 10: VPN-Profileinstellung	Beschreibung
	Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.
Sekundäres Kennwort	Diese Einstellung legt das Kennwort fest, das ein BlackBerry 10-Gerät für die Sekundär-Authentifizierung mit dem VPN-Gateway verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Cisco AnyConnect" gesetzt ist. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.
Gruppenname	Diese Einstellung legt den Gruppennamen für das VPN-Gateway fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Cisco AnyConnect" gesetzt ist. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.
Persönliche Apps in geschäftlichen Netzwerken zulassen	Diese Einstellung legt fest, ob persönliche Apps auf einem BlackBerry 10-Gerät eine VPN-Verbindung verwenden können. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Cisco AnyConnect“ gesetzt ist, und wenn die IT-Richtlinienregel „Persönlichen Apps die Verwendung von Geschäftsnetzwerken erlauben“ ausgewählt ist. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.
Automatische Client-Zertifikatsverarbeitung aktivieren	Diese Einstellung legt fest, ob ein Client-Zertifikat automatisch ausgewählt wird, wenn eine VPN-Verbindung hergestellt wird. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Cisco AnyConnect" gesetzt ist. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.
IPsec-Authentifizierung aktivieren	Diese Einstellung legt fest, ob das VPN-Gateway die IPsec-Authentifizierung verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Cisco AnyConnect" gesetzt ist. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.
IPsec-Authentifizierungstyp	Diese Einstellung legt den Authentifizierungstyp für eine IPsec VPN-Verbindung fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „IPsec-Authentifizierung aktivieren“ ausgewählt ist. Mögliche Werte:

BlackBerry 10: VPN-Profileinstellung	Beschreibung
	• EAP-MS-CHAPv2 • EAP-MD5 • EAP-GTC • EAP-AnyConnect • IKE-RSA Der Standardwert ist EAP-MS-CHAPv2. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.
EAP-Authentifizierungs-ID	Diese Einstellung legt die EAP-Identität fest, die ein BlackBerry 10-Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „IPsec-Authentifizierungstyp“ auf „EAP MSCHAPv2“, „EAP MD5“ oder „EAP GTC“ gesetzt ist.
Subnetze ausschließen	Diese Einstellung legt fest, ob bestimmte Subnetze von der Verwendung der VPN-Verbindung ausgenommen werden. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Cisco AnyConnect" gesetzt ist. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.
Ausgeschlossene Subnetze	Diese Einstellung legt die Subnetze und die Subnetzmasken fest, die nicht über die VPN-Verbindung gesendet werden. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Subnetzmarkierung deaktivieren“ ausgewählt ist.
Cisco AnyConnect-Konfigurationsdatei (.xml)	Diese Einstellung legt den Speicherort der Cisco AnyConnect-Konfigurationsdatei fest, die an BlackBerry 10-Geräte gesendet wird. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Cisco AnyConnect" gesetzt ist. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.
IP automatisch ermitteln	Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät die IP-Konfiguration des VPN-Gateways automatisch ermittelt.
Private IP	Diese Einstellung legt die private IP des VPN-Gateways fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „IP automatisch ermitteln“ nicht ausgewählt ist.

BlackBerry 10: VPN-Profileinstellung	Beschreibung
Private IP-Maske	Diese Einstellung legt die private IP-Maske des VPN-Gateways fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „IP automatisch ermitteln“ nicht ausgewählt ist.
Subnetz	Diese Einstellung legt das Subnetz des VPN-Gateways fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „IP automatisch ermitteln“ nicht ausgewählt ist.
Subnetzmaske	Diese Einstellung legt die Subnetzmaske des VPN-Gateways fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „IP automatisch ermitteln“ nicht ausgewählt ist.
DNS automatisch ermitteln	Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät die DNS-Konfiguration des VPN-Gateways automatisch ermittelt.
Primärer DNS	Diese Einstellung legt den primären DNS-Server in Dezimalschreibweise mit Punkt fest (beispielsweise „192.0.2.0“). Diese Einstellung ist nur dann gültig, wenn die Einstellung „DNS automatisch ermitteln“ nicht ausgewählt ist.
Sekundärer DNS	Diese Einstellung legt den sekundären DNS-Server in Dezimalschreibweise mit Punkt fest (beispielsweise „192.0.2.0“). Diese Einstellung ist nur dann gültig, wenn die Einstellung „DNS automatisch ermitteln“ nicht ausgewählt ist.
Domänensuffix	Diese Einstellung legt den FQDN des DNS-Suffixes fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „DNS automatisch ermitteln“ nicht ausgewählt ist.
Perfekte Geheimhaltung bei der Weiterleitung	Diese Einstellung legt fest, ob das VPN-Gateway PFS unterstützt. Wenn diese Einstellung ausgewählt ist, darf die Einstellung „IKE IPSec DH-Gruppe“ nicht auf „0“ gesetzt werden.
Manuelle Algorithmusauswahl	Diese Einstellung legt fest, ob Sie die kryptografischen Algorithmen für das VPN-Gateway einrichten müssen.
IKE DH-Gruppe	Diese Einstellung gibt die DH-Gruppe an, die ein BlackBerry 10-Gerät zur Generierung des Schlüssels verwendet.

BlackBerry 10: VPN-Profileinstellung	Beschreibung
	Diese Einstellung ist nur dann gültig, wenn die Einstellung „Manuelle Algorithmenauswahl“ ausgewählt ist. Mögliche Werte: • 1 bis 26 außer 3, 4 und 6 • Benutzerdefiniert 1 bis Benutzerdefiniert 5 Der Standardwert ist „1“.
Anbieter des benutzerdefinierten IKE DH	Diese Einstellung legt den Namen des Providers für die benutzerdefinierte IKE DH fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „IKE DH-Gruppe“ auf einen der benutzerdefinierten Werte gesetzt ist.
MOBIKE aktivieren	Diese Einstellung legt fest, ob das VPN-Gateway MOBIKE unterstützt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Microsoft IKEv2 VPN-Server“ oder „Generischer IKEv2 VPN-Server“ gesetzt ist oder wenn die Einstellung „Authentifizierungstyp“ auf „PKI“ und die Einstellung für die „IKE DH-Gruppe“ auf einen der benutzerdefinierten Werte gesetzt ist. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.
IKE-Chiffrierschlüssel	Diese Einstellung legt den Algorithmus fest, den ein BlackBerry 10-Gerät verwendet, um einen gemeinsam verwendeten geheimen Schlüssel zu generieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Manuelle Algorithmenauswahl“ ausgewählt ist. Mögliche Werte: • Keine • DES (56-Bit-Schlüssel) • Triple DES (168-Bit-Schlüssel) • AES (128-Bit-Schlüssel) • AES (192-Bit-Schlüssel) • AES (256-Bit-Schlüssel) Der Standardwert ist „Keine“.
IKE-Hash	Diese Einstellung legt die Hash-Funktion fest, die ein BlackBerry 10-Gerät mit IKE verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Manuelle Algorithmenauswahl“ ausgewählt ist.

BlackBerry 10: VPN-Profileinstellung	Beschreibung
	Mögliche Werte: • Keine • MD5 • AES-XCBC • SHA-1 • SHA-256 • SHA-384 • SHA-512 Der Standardwert ist „Keine“.
IKE PRF	Diese Einstellung legt die PRF-Funktion fest, die ein BlackBerry 10-Gerät mit IKE verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Manuelle Algorithmenauswahl“ ausgewählt ist. Mögliche Werte: • Keine • HMAC • HMAC-MD5 • AES-XCBC • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512 Der Standardwert ist „Keine“.
IPsec DH-Gruppe	Diese Einstellung legt die DH-Gruppe fest, die ein BlackBerry 10-Gerät mit IPsec verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Manuelle Algorithmenauswahl“ ausgewählt ist. Mögliche Werte sind 0 bis 26 außer 3, 4 und 6. Der Standardwert ist „0“.
IPsec-Chiffrierschlüssel	Diese Einstellung legt den Algorithmus fest, den ein BlackBerry 10-Gerät mit IPsec verwendet.

BlackBerry 10: VPN-Profileinstellung	Beschreibung
	Diese Einstellung ist nur dann gültig, wenn die Einstellung „Manuelle Algorithmenauswahl“ ausgewählt ist. Mögliche Werte: • Keine • DES (56-Bit-Schlüssel) • Triple DES (168-Bit-Schlüssel) • AES (128-Bit-Schlüssel) • AES (192-Bit-Schlüssel) • AES (256-Bit-Schlüssel) Der Standardwert ist „Keine“.
IPsec-Hash	Diese Einstellung legt die Hash-Funktion fest, die ein BlackBerry 10-Gerät mit IPsec verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Manuelle Algorithmenauswahl“ ausgewählt ist. Mögliche Werte: • Keine • MD5 • AES-XCBC • SHA-1 • SHA-256 • SHA-384 • SHA-512 Der Standardwert ist „Keine“.
IKE-Lebensdauer	Diese Einstellung legt die Lebensdauer der IKE-Verbindung in Sekunden fest. Wenn Sie einen nicht unterstützten Wert oder einen Nullwert setzen, wird der Standardwert des BlackBerry 10-Geräts verwendet. Mögliche Werte sind 1 bis 2.147.483.647.
IPsec-Lebensdauer	Diese Einstellung legt die Lebensdauer der IPsec-Verbindung in Sekunden fest. Wenn Sie einen nicht unterstützten Wert oder einen Nullwert setzen, wird der Standardwert des BlackBerry 10-Geräts verwendet.

BlackBerry 10: VPN-Profileinstellung	Beschreibung
	Mögliche Werte sind 1 bis 2.147.483.647.
NAT-Keepalive	Diese Einstellung legt fest, wie häufig ein Gerät ein NAT-Keep-alive-Paket sendet. Wenn Sie einen nicht unterstützten Wert oder einen Nullwert setzen, wird der Standardwert des BlackBerry 10-Geräts verwendet. Mögliche Werte sind 1 bis 2.147.483.647.
DPD-Häufigkeit	Diese Einstellung legt die DPD-Frequenz in Sekunden fest. Ein BlackBerry 10-Gerät unterstützt eine Mindesteinstellung von 10 Sekunden. Wenn Sie einen nicht unterstützten Wert oder einen Nullwert setzen, wird der Standardwert des Geräts verwendet. Mögliche Werte sind 1 bis 2.147.483.647.
Split-Tunneling	Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät Split-Tunneling verwenden kann, um das VPN-Gateway zu umgehen, sofern vom VPN-Gateway unterstützt.
Banner deaktivieren	Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät das VPN-Banner blockiert.
Benutzerdefinierbar	Dieses Feld gibt dieVPN-Funktionen an, die ein BlackBerry 10-Gerätebenutzer ändern kann. Wenn diese Einstellung auf „Schreibgeschützt“ gesetzt ist, kann der Benutzer keine Einstellung ändern. Wenn diese Einstellung auf „Nur Anmeldedaten“ gesetzt ist, kann der Benutzer den Benutzernamen und das Kennwort ändern. Mögliche Werte: • Schreibgeschützt • Nur Anmeldedaten Der Standardwert ist „Schreibgeschützt“.
VPN-Informationen auf Gerät anzeigen	Diese Einstellung legt fest, ob VPN-Informationen auf einem BlackBerry 10-Gerät angezeigt werden. Wenn diese Einstellung auf „Sichtbar“ gesetzt ist, werden die meisten Informationen des VPN-Profils auf dem Gerät angezeigt. Wenn diese Einstellung auf „Unsichtbar“ gesetzt ist, wird nur der Profilname auf dem Gerät angezeigt. Wenn diese Einstellung auf „Nur Anmeldedaten“ gesetzt ist, werden nur die Felder für den Profilnamen und die Anmeldeinformationen auf dem Gerät angezeigt. Mögliche Werte: • Sichtbar • Nicht sichtbar • Nur Anmeldedaten Der Standardwert ist „Sichtbar“.

BlackBerry 10: VPN-Profileinstellung	Beschreibung
Quelle des Client-Zertifikats	Diese Einstellung legt fest, wie BlackBerry 10-Geräte das Client-Zertifikat abrufen können. Für den Abruf von Client-Zertifikaten über die Geräte stehen vier Möglichkeiten zur Verfügung: • Wenn Sie „SCEP“ wählen, müssen Sie auch das verknüpfte SCEP-Profil festlegen, das vom Gerät verwendet werden kann, um das Client-Zertifikat herunterzuladen. • Wenn Sie „Benutzeranmeldeinformationen“ wählen, müssen Sie auch das Profil für Benutzeranmeldeinformationen festlegen, das das Gerät verwenden kann, um das Client-Zertifikat herunterzuladen. • Wenn Sie „Smartcard“ wählen, muss der Benutzer das Gerät mit einer Smartcard pairen, die das Client-Zertifikat enthält. • Wenn Sie „Sonstiges“ wählen, muss der Benutzer das Client-Zertifikat manuell zum Gerät hinzufügen. Smartcard-Unterstützung steht für Geräte zur Verfügung, auf denen BlackBerry 10 OS Version 10.3.1 oder höher ausgeführt wird. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „PKI“ oder „XAUTH-PKI“ gesetzt ist. Mögliche Werte: • Smartcard • SCEP • Benutzeranmeldeinformationen • Anderes Der Standardwert ist „Sonstiges“.
Verknüpftes SCEP-Profil	Diese Einstellung legt das verknüpfte SCEP-Profil fest, das ein BlackBerry 10-Gerät verwendet, um ein Client-Zertifikat für die VPN-Authentifizierung abzurufen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Quelle des Client-Zertifikats“ auf „SCEP“ gesetzt ist.
Verknüpftes Profil für Benutzeranmelde-informationen	Diese Einstellung legt das verknüpfte Profil für Benutzeranmeldeinformationen fest, das ein BlackBerry 10-Gerät verwendet, um ein Client-Zertifikat für die Authentifizierung mit dem VPN abzurufen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Quelle des Client-Zertifikats“ auf „Benutzeranmeldeinformationen“ gesetzt ist. Die Mindestanforderung für die Verwendung eines Profils für Benutzeranmeldeinformationen ist BlackBerry 10 OS-Version 10.31.

BlackBerry 10: VPN-Profileinstellung	Beschreibung
Aktion bei nicht vertrauenswürdigem Zertifikat	Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät nicht vertrauenswürdige Zertifikate annimmt. Wenn die Einstellung auf „Zulassen“ gesetzt ist, nimmt das Gerät nicht vertrauenswürdige Zertifikate automatisch an. Wenn die Einstellung auf „Eingabeaufforderung“ gesetzt ist, kann der Benutzer entscheiden, ob er nicht vertrauenswürdige Zertifikate annehmen möchte. Wenn diese Einstellung auf „Nicht zulassen“ gesetzt ist, lehnt das Gerät nicht vertrauenswürdige Zertifikate ab. Die Einstellung „Gatewaytyp“ legt fest, welche nicht vertrauenswürdigen Zertifikataktionen unterstützt werden und welcher Standardwert für diese Einstellung verwendet wird. Mögliche Werte: • Zulassen • Eingabeaufforderung • Nicht zulassen Die Mindestanforderung ist BlackBerry 10 OS-Version 10.32
Quelle des vertrauenswürdigen Zertifikats	Diese Einstellung legt die Quelle des vertrauenswürdigen Zertifikats fest. Wenn diese Einstellung auf „Speicher für vertrauenswürdige Zertifikate“ gesetzt ist, kann ein BlackBerry 10-Gerät eine Verbindung zu einem VPN aufbauen, das ein beliebiges Zertifikat im VPN-Zertifikatspeicher verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „PKI“ oder „XAUTH-PKI“ gesetzt ist. Mögliche Werte: • Keine • Speicher vertrauenswürdiger Zertifikate Der Standardwert ist „Keine“.
Datensicherheitsstufe	Diese Einstellung legt die Domäne im geschäftlichen Bereich fest, in der das VPN-Profil gespeichert ist, wenn der geschäftliche Bereich mit erweitertem Schutz von Daten im Ruhestand arbeitet. Diese Einstellung ist nur dann gültig, wenn die IT-Richtlinienregel „Erweiterten Schutz von Daten im Ruhestand erzwingen“ ausgewählt ist. Wenn diese Einstellung auf „Immer verfügbar“ gesetzt ist, wird das Profil in der Startdomäne gespeichert und steht zur Verfügung, wenn der geschäftliche Bereich gesperrt ist. Wenn diese Einstellung auf „Verfügbar nach Authentifizierung“ gesetzt ist, wird das Profil in der Betriebsdomäne gespeichert und ist nach dem Entsperren des geschäftlichen Bereichs so lange verfügbar, bis das Gerät erneut gestartet wird. Wenn diese Einstellung auf „Nur verfügbar, wenn der geschäftliche Bereich entsperrt ist“ gesetzt ist, wird das Profil in der Sperrdomäne gespeichert

BlackBerry 10: VPN-Profileinstellung	Beschreibung
	und kann nur dann für VPN-Verbindungen verwendet werden, wenn der geschäftliche Bereich entsperrt ist. Mögliche Werte: • Immer verfügbar • Verfügbar nach Authentifizierung • Nur verfügbar, wenn der geschäftliche Bereich entsperrt ist Der Standardwert ist „Immer verfügbar“. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.
Verknüpftes Proxy-Profil	Diese Einstellung legt das verknüpfte Proxy-Profil fest, das ein BlackBerry 10-Gerät verwendet, um eine Verbindung zu einem Proxy-Server aufzubauen, wenn das Gerät mit dem VPN verbunden ist.

iOS: VPN-Profileinstellungen

iOS: VPN-Profileinstellung	Beschreibung
Verbindungstyp	Diese Einstellung legt den Verbindungstyp fest, den ein iOS-Gerät für ein VPN-Gateway verwendet. Bei einigen Verbindungstypen müssen die Benutzer außerdem die entsprechende VPN-App auf dem Gerät installieren. Mögliche Werte: • L2TP • PPTP • IPSec • Cisco AnyConnect • Juniper • F5 • SonicWALL Mobile Connect • Aruba VIA • Check Point Mobile • OpenVPN • Benutzerdefiniert

iOS: VPN-Profileinstellung	Beschreibung
	Der Standardwert ist „L2TP“.
VPN-Bundle-ID	Diese Einstellung legt die Bundle-ID der VPN-App für ein benutzerdefiniertes SSL-VPN fest. Die Bundle-ID wird im umgekehrten DNS-Format angegeben (beispielsweise „com.example.VPNapp“). Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „Benutzerdefiniert“ gesetzt ist.
Server	Diese Einstellung legt den FQDN oder die IP-Adresse eines VPN-Servers fest.
Benutzername	Diese Einstellung legt den Benutzernamen fest, den ein iOS-Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren. Wenn das Profil für mehrere Benutzer gilt, können Sie die %UserName%-Variable angeben.
Benutzerdefinierte Schlüsselwertepaare	Diese Einstellung legt die Schlüssel und die verknüpften Werte für das benutzerdefinierte SSL-VPN fest. Die Konfigurationsinformationen sind spezifisch für die VPN-App des Anbieters. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „Benutzerdefiniert“ gesetzt ist.
Anmeldegruppe oder Domäne	Diese Einstellung legt die Anmeldegruppe oder -domäne fest, die das VPN-Gateway verwendet, um ein iOS-Gerät zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „SonicWALL Mobile Connect“ gesetzt ist.
Bereich	Diese Einstellung legt den Namen des Authentifizierungsbereichs fest, den das VPN-Gateway verwendet, um ein iOS-Gerät zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „Juniper“ gesetzt ist.
Aufgabenbereich	Diese Einstellung legt den Namen der Benutzerrolle fest, den ein VPN-Gateway verwendet, um die Netzwerkressourcen zu überprüfen, auf die ein iOS-Gerät zugreifen kann. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „Juniper“ gesetzt ist.
Authentifizierungstyp	Diese Einstellung legt den Authentifizierungstyp für das VPN-Gateway fest. Die Einstellung „Verbindungstyp“ legt fest, welche Authentifizierungstypen unterstützt werden und welcher Standardwert für diese Einstellung verwendet wird. Mögliche Werte:

iOS: VPN-Profileinstellung	Beschreibung
	• Kennwort • RSA SecurID • Gemeinsamer geheimer Schlüssel/Gruppenname • Freigegebenes Zertifikat • SCEP • Benutzeranmeldeinformationen
Kennwort	Diese Einstellung legt das Kennwort fest, das ein iOS-Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Kennwort“ gesetzt ist.
Gruppenname	Diese Einstellung legt den Gruppennamen für das VPN-Gateway fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „Cisco AnyConnect“ gesetzt ist, oder wenn die Einstellung „Verbindungstyp“ auf „IPsec“ und die Einstellung „Authentifizierungstyp“ auf „Gemeinsamer geheimer Schlüssel/Gruppenname“ gesetzt sind.
Gemeinsamer geheimer Schlüssel	Diese Einstellung legt den gemeinsamen geheimen Schlüssel für das VPN-Gateway fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „L2TP“ gesetzt ist, oder wenn die Einstellung „Verbindungstyp“ auf „IPsec“ und die Einstellung „Authentifizierungstyp“ auf „Gemeinsamer geheimer Schlüssel/Gruppenname“ gesetzt sind.
Profil für freigegebenes Zertifikat	Diese Einstellung legt das Profil für das freigegebene Zertifikat mit dem Client-Zertifikat fest, das ein iOS-Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Freigegebenes Zertifikat“ gesetzt ist.
Verknüpftes SCEP-Profil	Diese Einstellung legt das verknüpfte SCEP-Profil fest, das ein iOS-Gerät verwendet, um ein Client-Zertifikat für die VPN-Authentifizierung abzurufen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „SCEP“ gesetzt ist.
Verknüpftes Profil für Benutzeranmelde-informationen	Diese Einstellung legt das verknüpfte Profil für Benutzeranmeldeinformationen fest, das ein iOS-Gerät verwendet, um ein Client-Zertifikat für die Authentifizierung mit dem VPN abzurufen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Benutzeranmeldeinformationen“ gesetzt ist.

iOS: VPN-Profileinstellung	Beschreibung
Verschlüsselungsstufe	Diese Einstellung legt die Stufe der Datenverschlüsselung für die VPN-Verbindung fest. Wenn diese Einstellung auf „Automatisch“ gesetzt ist, sind alle verfügbaren Verschlüsselungsstärken zulässig. Wenn diese Einstellung auf „Maximum“ gesetzt ist, ist nur die maximale Verschlüsselungsstärke zulässig. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „PPTP“ gesetzt ist. Mögliche Werte: • Keine • Automatisch • Maximum Der Standardwert ist „Keine“.
Netzwerkverkehr durch VPN leiten	Diese Einstellung legt fest, ob der gesamte Netzwerkverkehr durch die VPN-Verbindung gesendet werden soll. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „L2TP“ oder „PPTP“ gesetzt ist.
Hybrid-Authentifizierung verwenden	Diese Einstellung legt fest, ob ein serverseitiges Zertifikat für die Authentifizierung verwendet wird. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IPsec“ und der „Authentifizierungstyp“ auf „Gemeinsamer geheimer Schlüssel/Gruppenname“ gesetzt ist.
Zur Kennworteingabe auffordern	Diese Einstellung legt fest, ob ein iOS-Gerät den Benutzer zur Eingabe eines Kennworts auffordert. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IPsec“ und der „Authentifizierungstyp“ auf „Gemeinsamer geheimer Schlüssel/Gruppenname“ gesetzt ist.
Zur PIN-Eingabe auffordern	Diese Einstellung legt fest, ob das iOS-Gerät den Benutzer zur Eingabe einer PIN auffordert. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IPsec“ gesetzt ist, und die Einstellung für den „Authentifizierungstyp“ auf „Freigegebenes Zertifikat“, „SCEP“ oder „Benutzeranmeldeinformationen“ gesetzt ist.
VPN bei Bedarf aktivieren	Diese Einstellung legt fest, ob ein Gerät automatisch beim Zugriff auf bestimmte Domänen eine VPN-Verbindung herstellen kann. Diese Einstellung betrifft geschäftliche Apps.

iOS: VPN-Profileinstellung	Beschreibung
	Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IPsec“, „Cisco AnyConnect“, „Juniper“, „F5“, „SonicWALL Mobile Connect“, „Aruba VIA“, „Check Point Mobile“, „OpenVPN“ oder „Benutzerdefiniert“ gesetzt ist und der „Authentifizierungstyp“ auf „Freigegebenes Zertifikat“, „SCEP“ oder „Benutzeranmeldeinformationen“ gesetzt ist.
Domänen- oder Hostnamen, die "VPN auf Abruf" verwenden können	Diese Einstellung legt die Domänen und die verknüpften Aktionen für VPN bei Bedarf fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN bei Bedarf aktivieren“ ausgewählt ist. Mögliche Werte für die „Bei Bedarf-Aktion“: • Immer herstellen • Herstellen, wenn erforderlich • Niemals herstellen
Regeln für „VPN bei Bedarf“ für iOS 7.0 und höher	Diese Einstellung legt die Verbindungsanforderungen für VPN bei Bedarf fest. Sie müssen einen oder mehrere Schlüssel aus dem Beispiel für das Nutzlastformat verwenden. Diese Einstellung überschreibt die Einstellung „Domänen- oder Hostnamen, die VPN bei Bedarf verwenden können“. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN bei Bedarf aktivieren“ ausgewählt ist.
Per App VPN aktivieren	Diese Einstellung legt fest, ob das VPN-Gateway Per App VPN unterstützt. Mit dieser Funktion kann die Belastung im VPN einer Organisation reduziert werden. So könnten Sie beispielsweise festlegen, dass nur ein bestimmter geschäftlicher Datenverkehr, wie etwa der Zugriff auf Anwendungsserver oder Webseiten, über das VPN abgewickelt wird. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „Cisco AnyConnect“, „Juniper“, „F5“, „SonicWALL Mobile Connect“, „Aruba VIA“, „Check Point Mobile“, „OpenVPN“ oder „Benutzerdefiniert“ gesetzt ist.
Safari-Domänen	Diese Einstellung legt die Domänen fest, die die VPN-Verbindung in Safari starten können. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Per App VPN aktivieren“ ausgewählt ist.
Zulassen, dass Apps automatisch eine Verbindung herstellen	Diese Einstellung legt fest, ob mit Per App VPN verknüpfte Apps die VPN-Verbindung automatisch starten können. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Per App VPN aktivieren“ ausgewählt ist.

iOS: VPN-Profileinstellung	Beschreibung
Verknüpftes Proxy-Profil	Diese Einstellung legt das verknüpfte Proxy-Profil fest, das ein iOS-Gerät verwendet, um eine Verbindung zu einem Proxy-Server aufzubauen, wenn das Gerät mit dem VPN verbunden ist.

Android: VPN-Profileinstellungen

VPN-Profile werden nur von Samsung KNOX Workspace-Geräten unterstützt.

Zur Verwendung von VPN-Profilen müssen Geräte mit der Aktivierungsart „Geschäftlich und persönlich – vollständige Kontrolle (Samsung KNOX)“ oder „Nur geschäftlicher Bereich (Samsung KNOX)“ aktiviert werden.

Android: VPN-Profileinstellung	Beschreibung
Serveradresse	Diese Einstellung legt den FQDN oder die IP-Adresse eines VPN-Servers fest.
VPN-Typ	Diese Einstellung legt fest, ob ein Gerät IPsec oder SSL verwendet, um eine Verbindung mit dem Mailserver aufzubauen. Mögliche Werte: • IPSec • SSL Der Standardwert ist „IPsec“. Der Juniper-VPN-App unterstützt nur SSL.
Benutzerauthentifizierung erforderlich	Diese Einstellung legt fest, ob ein Gerät einen Benutzernamen und ein Kennwort zum Herstellen einer Verbindung mit dem VPN-Server bereitstellen muss.
Benutzername	Diese Einstellung legt den Benutzernamen fest, den ein Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren. Wenn das Profil für mehrere Benutzer gilt, können Sie die %UserName%-Variable verwenden. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Benutzerauthentifizierung erforderlich“ ausgewählt wurde.
Kennwort	Diese Einstellung legt das Kennwort fest, den ein Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Benutzerauthentifizierung erforderlich“ ausgewählt wurde.
Split-Tunnel-Typ	Diese Einstellung legt fest, ob ein Gerät Split-Tunneling verwenden kann, um das VPN-Gateway zu umgehen, sofern dies vom VPN-Gateway unterstützt wird. Mögliche Werte:

Android: VPN-Profileinstellung	Beschreibung
	• Deaktiviert • Manuell • Automatisch Wenn der VPN-Typ auf „IPsec“ festgelegt ist, muss diese Einstellung auf „Deaktiviert“ festgelegt werden. Der Standardwert ist „Deaktiviert“.
Weiterleitungsrouten	Diese Einstellung legt die Route(n) zum Umgehen des VPN-Gateways fest. Sie können eine oder mehrere IP-Adressen angeben. Diese Einstellung ist nur dann gültig, wenn „VPN-Typ“ auf „SSL“ und der „Split-Tunnel-Typ“ auf „Manuell“ gesetzt ist.
DPD	Diese Einstellung legt fest, ob DPD aktiviert ist. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
IKE-Version	Diese Einstellung gibt die Version des IKE-Protokolls zur Verwendung mit der VPN-Verbindung an. Mögliche Werte: • IKEv1 • IKEv2 Der Standardwert ist „IKEv1“. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
IPsec-Authentifizierungstyp	Diese Einstellung legt den Authentifizierungstyp für die IPsec-VPN-Verbindung fest. Die Einstellung „IKE-Version“ legt fest, welche IPsec-Authentifizierungstypen unterstützt werden und welcher Standardwert für diese Einstellung verwendet wird. Mögliche Werte: • Zertifikat • Preshared key • Hybrid RSA • CAC-basierte Authentifizierung Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.

Android: VPN-Profileinstellung	Beschreibung
ID-Typ der IPsec-Gruppe	Diese Einstellung legt den IPsec-Gruppen-ID-Typ für die VPN-Verbindung fest. Die Einstellung „IPsec-Authentifizierungstyp“ legt fest, welche IPsec-Gruppen-ID-Typen unterstützt werden und welcher Standardwert für diese Einstellung verwendet wird. Mögliche Werte: • Standard • IPv4-Adresse • Fully Qualified Domain Name (vollständiger Domänenname) • Benutzer-FQDN • IKE-Schlüssel-ID Wird für „IPsec-Authentifizierungstyp“ die Einstellung „Zertifikat“ verwendet, dann wird diese Einstellung automatisch auf „Standard“ festgelegt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
IPsec-Gruppen-ID	Diese Einstellung legt die IPsec-Gruppen-ID für die VPN-Verbindung fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
Schlüsselaustauschmodus IKE-Phase-1	Diese Einstellung legt den Austauschmodus für die VPN-Verbindung fest. Mögliche Werte: • Hauptmodus • Aggressive-Modus Der Standardwert ist „Hauptmodus“. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
IKE-Lebensdauer	Diese Einstellung legt die Lebensdauer der IKE-Verbindung in Sekunden fest. Wenn Sie einen nicht unterstützten Wert oder einen Nullwert setzen, wird der Standardwert des Geräts verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
IKE-Verschlüsselungsalgorithmus	Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
IKE-Integritätsalgorithmus	Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
IPsec DH-Gruppe	Diese Einstellung gibt die DH-Gruppe an, die ein Gerät zur Generierung des Schlüssels verwendet. Mögliche Werte sind 0, 1, 2, 5 und 14 bis 26.

Android: VPN-Profileinstellung	Beschreibung
	Der Standardwert ist 0. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
IPsec-Parameter	Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
Perfekte Geheimhaltung bei der Weiterleitung	Diese Einstellung legt fest, ob das VPN-Gateway PFS unterstützt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
MOBIKE aktivieren	Diese Einstellung legt fest, ob das VPN-Gateway MOBIKE unterstützt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
IPsec-Lebensdauer	Diese Einstellung legt die Lebensdauer der IPsec-Verbindung in Sekunden fest. Wenn Sie einen nicht unterstützten Wert oder einen Nullwert setzen, wird der Standardwert des Geräts verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
IPsec-Verschlüsselungsalgorithmus	Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
IPsec-Integritätsalgorithmus	Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
Authentifizierungstyp	Diese Einstellung legt den Authentifizierungstyp für das VPN-Gateway fest. Mögliche Werte: • Keine • Zertifikatsbasierte Authentifizierung • CAC-basierte Authentifizierung Der Standardwert ist „Keine“. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „SSL“ gesetzt ist.
SSL-Algorithmus	Diese Einstellung gibt den für eine SSL-VPN-Verbindung erforderlichen Verschlüsselungsalgorithmus an. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „SSL“ gesetzt ist.
UID-/PID-Informationen anhängen	Diese Einstellung gibt an, ob UID/PID-Informationen an Pakete angehängt werden, die an den VPN-Client gesendet werden. Diese Einstellung muss für die Cisco AnyConnect VPN-App aktiviert werden.

Android: VPN-Profileinstellung	Beschreibung
Verkettung unterstützen	Diese Einstellung legt fest, wie die VPN-Verkettung unterstützt wird. Mögliche Werte: • Verkettung unterstützen • Äußerer Tunnel • Innerer Tunnel Der Standardwert ist „Verkettung unterstützen“.
Schlüsselwertpaare des Anbieters	Diese Einstellung legt die Schlüssel und die verknüpften Werte für das VPN fest. Die Konfigurationsinformationen sind spezifisch für die VPN-App des Anbieters.
Paket-ID des VPN-Clients	Diese Einstellung legt die Paket-ID der VPN-App fest.
Verbindung nach Fehler automatisch wiederherstellen	Diese Einstellung legt fest, ob die VPN-Verbindung nach Verbindungsverlust automatisch neu hergestellt werden soll.
FIPS-Modus aktivieren	Diese Einstellung legt fest, ob FIPS aktiviert ist. Durch Aktivieren des FIPS-Modus wird sichergestellt, dass nur FIPS-geprüfte Kryptografiealgorithmen für die VPN-Verbindung verwendet werden.

Unterstützte Leistungsmerkmale nach Gerätetyp

Vergleich der unterstützten Funktionen nach Gerätetyp

Multiplatform

Unterstützte Leistungsmerkmale nach Gerätetyp

35

In dieser Kurzanleitung werden die in BES12 Version 12.2 unterstützten Funktionen von Geräten mit BlackBerry 10, BlackBerry OS (Version 5.0 bis 7.1), iOS, Android und Windows Phone miteinander verglichen.

Die Unterstützung von BlackBerry OS-Geräten erfordert ein Upgrade von BES5 aufBES12.

Aktuelle Informationen zur Betriebssystemkompatibilität finden Sie in der Kompatibilitätsmatrix in der Dokumentation zu Installation und Upgrade unter help.blackberry.com/detectLang/bes12/.

Gerätefunktionen

Funktion	BlackBerry 10	BlackBerry OS	iOS	Android	Windows Phone
Für die Aktivierung ist erforderlich, dass auf dem Gerät eine Client-App oder ein Client-Konto eingerichtet wird			√	√	√
Trennung von geschäftlichen und persönlichen Daten	√	√	√ *	√ *	
Benutzer-Datenschutz für persönliche Daten	√	√	√ *	√ *	
Verschlüsselung von geschäftlichen Daten im Ruhezustand	√	√	√ *	√ *	
Sperren des Zugriffs auf geschäftliche Daten nach einem Zeitraum der Inaktivität	√	√	√	√	√
Löschen von geschäftlichen Daten nach einem Zeitraum der Inaktivität	√		√ *	√ *	

Funktion	BlackBerry 10	BlackBerry OS	iOS	Android	Windows Phone
Schutz von Geräten durch Senden von IT-Befehlen	√	√	√	√	√
Steuern von Gerätefunktionen mithilfe von IT-Richtlinien	√	√	√	√	√
Erzwingen der Verschlüsselung von Medienkarten	√	√		√	

* Für iOS-Geräte und Android-Geräte, die Android for Work nicht verwenden, ist eine Gold - Secure Work Space-Server-Lizenz oder eine Gold SIM-Lizenz erforderlich.

Anzeigen von Gerätedetails

Funktion	BlackBerry 10	BlackBerry OS	iOS	Android	Windows Phone
Geräteeigentümer	√	√	√	√	√
Benutzername, E-Mail-Adresse und Telefonnummer	√	√	√	√	√
Aktivierungsstatus, Aktivierungsdatum, letzter Kontakt	√	√	√	√	√
Mobilfunkanbieter	√	√	√	√	√
Hardware-Details (CPU, RAM, verfügbarer Hauptspeicher und Speicherplatz)	√	√	√	√	√
Netzwerkdetails (IP, MAC, VPN, Wi-Fi, Sicherheitsprotokolle)	√		√	√	√

Funktion	BlackBerry 10	BlackBerry OS	iOS	Android	Windows Phone
Hardwarefunktionen (Bluetooth-Version, GPS, Kamera, Akku-Ladezustand, Gyroskop, Formfaktor, Abmessungen)	√		√	√	√
OS-Typ und -Version	√	√	√	√	√
Vorschriftenverletzungsstatus	√		√	√	√
Auf Gerät angewendete Profile	√	√	√	√	√
Vorhandensein einer Medienkarte und verfügbaren Speichers	√			√	√
Verschlüsselungsstatus der Medienkarte	√			√	√
Installationsstatus geschäftlicher Apps	√	√	√	√	√

Steuern von Geräten und Konfigurieren des Gerätezugriffs auf das Unternehmensnetzwerk

Funktion	BlackBerry 10	BlackBerry OS	iOS	Android	Windows Phone
IT-Richtlinien	√	√	√	√	√
Exchange ActiveSync E-Mail-Profile	√		√	√ *	√
IMAP/POP3 E-Mail-Profile			√	√	√
Aktivierungsprofile	√		√	√	√
Profile, die Enterprise-	√		√	√	

Funktion	BlackBerry 10	BlackBerry OS	iOS	Android	Windows Phone
Konnektivität bereitstellen					
Wi-Fi-Profile	√	√	√	√	√
VPN-Profile	√	√	√	√ **	
Proxy-Profile	√		√	√	
Profile für die Vorschriften-einhaltung	√		√	√	√
Profile für die einmalige Anmeldung	√		√		
Profile für Zertifizierungsstellen-zertifikate	√		√	√	√
Profile für freigegebenes Zertifikat			√	√	
Profile für Benutzeranmelde-informationen	√		√	√	
SCEP-Profile	√		√	√	
Profile für App-Sperrmodus			√ ***	√ ***	
Andere OS-spezifische Profile	• Profil für Gerätedienst an-forderungen • Zertifikats-abrufprofile • OCSP-Profile • CRL-Profile	• Softwarekonfi-gurationen • Zugriffs-steuerungs-regeln	• Webinhalts-filter-Profile • Websymbol-Profile • Profile für die Standort-bestimmung		

Funktion	BlackBerry 10	BlackBerry OS	iOS	Android	Windows Phone
			• Profile mit verwalteten Domänen		

* Nur bei Geräten, auf denen TouchDown installiert ist, Motorola-Geräten, die die EDM API unterstützen, Geräten mit Android for Work oder Geräten, die Samsung KNOX mit Exchange ActiveSync verwenden.

** Nur bei KNOX Workspace-Geräten

*** Nur bei überwachten iOS-Geräten, die MDM-Steuerelemente verwenden, und Android-Geräten, die KNOX MDM verwenden.

Schützen von verlorenen oder gestohlenen Geräten

Funktion	BlackBerry 10	BlackBerry OS	iOS	Android	Windows Phone
Angeben des Gerätekennworts	√	√		√	√
Sperren des Geräts	√	√	√	√	√
Entsperren des Geräts und Löschen des Kennworts			√	√	
Alle Gerätedaten löschen	√	√	√	√ *	√
Nur Löschen von Geschäftsdaten	√	√	√	√	√

* Bei Motorola Geräten, die die EDM API unterstützen, werden Daten auf der Medienkarte ebenfalls gelöscht. Bei Geräten mit Samsung KNOX Workspace können Sie optional ebenfalls die Daten auf der Medienkarte löschen.

Konfigurieren des Roaming

Funktion	BlackBerry 10	BlackBerry OS	iOS	Android	Windows Phone
Deaktivieren der Synchronisation mit dem E-Mail-Server während des Roaming	√		√	√ *	

Funktion	BlackBerry 10	BlackBerry OS	iOS	Android	Windows Phone
Deaktivieren von Daten während des Roaming	√			√ *	√

Nur bei Geräten, die KNOX MDM verwenden

Apps verwalten

Funktion	BlackBerry 10	BlackBerry OS	iOS	Android	Windows Phone
Verteilen von öffentlichen Apps von der Verkaufsplattform (BlackBerry World, App Store, Google Play, Windows Phone Store)	√		√	√	√
Verwalten des Katalogs geschäftlicher Apps	√	√	√	√	√
Verteilen interner Apps	√	√	√	√ *	√
Stille Installation interner Apps	√	√	√	√ **	√

* Bei Android-Geräten mit Ausnahme solcher, die Android for Work verwenden

Nur bei Geräten, die Samsung KNOX verwenden

Weitere Informationen

Weitere Informationen zu BES12 finden Sie unter help.blackberry.com/detectLang/bes12/.

Richtlinien-Referenztabelle

Weitere Informationen über IT-Richtlinien finden Sie in der Richtlinien-Referenztabelle unter help.blackberry.com/detectLang/bes12/current/policy-reference-spreadsheet-zip/.

Secure

Produktdokumentation

Ressource	Beschreibung
Übersicht und neue Funktionen	• Einführung in BES12 und die zugehörigen Funktionen • Orientierungshilfe für die Dokumentation • Architektur • Beschreibung der BES12-Komponenten • Beschreibung der Aktivierung und anderer Datenflüsse, wie Konfigurationsupdates und E-Mail, für unterschiedliche Gerätetypen
Versionshinweise und Ratgeber	• Beschreibung von bekannten Problemen und potenziellen Workarounds
Installation und Upgrade	• Systemanforderungen • Planung der BES12-Bereitstellung für eine Installation oder ein Upgrade von BES5 oder BES10 • Installationsanweisungen • Upgrade-Anweisungen
Installation und Verwaltung	• Systemanforderungen • Installationsanweisungen • Grundlegende Verwaltung vonBlackBerry Collaboration Service-Instanzen • Beschreibung der BlackBerry Collaboration Service-Komponenten • Architektur
Konfiguration	• Beschreibungen der verschiedenen Lizenztypen • Anweisungen zur Aktivierung und Verwaltung von Lizenzen • Anweisungen zur Konfiguration von Serverkomponenten vor der Verwaltung von Benutzern und ihren Geräten • Anweisungen zur Migration von BES10-Daten aus einer bestehenden BES10-Datenbank

Ressource	Beschreibung
Verwaltung	• Grundlegende und erweitere Verwaltung aller unterstützten Gerätetypen, darunter Geräte mit BlackBerry 10, iOS, Android, Windows Phone und BlackBerry OS (Version 5.0 bis 7.1) und niedriger • Anweisungen zum Erstellen von Benutzerkonten, Gruppen, Rollen und Administratorkonten • Anweisungen zur Aktivierung von Geräten • Anweisungen zum Erstellen und Zuweisen von IT-Richtlinien und Profilen • Anweisungen zum Verwalten von Apps auf Geräten • Beschreibungen der Profileinstellungen • Beschreibungen der IT-Richtlinienregeln für Geräte mit BlackBerry 10, iOS, Android, Windows Phone und BlackBerry OS (Version 5.0 bis 7.1) und niedriger
Sicherheit	• Beschreibung der Sicherheit von BES12, der BlackBerry Infrastructure und BlackBerry 10-Geräten zum Schutz von Daten und Verbindungen • Beschreibung von BlackBerry 10 OS • Beschreibung des Schutzes geschäftlicher Daten auf BlackBerry 10-Geräten bei der Verwendung von BES12 • Beschreibung der Sicherheitsfunktionen von BES12, der BlackBerry Infrastructure sowie den in BES12 aktivierten iOS-, Android- und Windows Phone-Geräten zum Schutz von Daten im Ruhezustand und während der Übertragung • Beschreibung des Schutzes geschäftlicher Apps auf Geräten mit geschäftlichem Bereich bei Verwendung von BES12

Glossar

AES	Advanced Encryption Standard (erweiterter Verschlüsselungsstandard)
AET	Application Enrollment Token
APNs	Apple Push Notification service (Apple Push Notification-Dienst)
BES5	BlackBerry Enterprise Server 5
BES10	BlackBerry Enterprise Service 10
BES12	BlackBerry Enterprise Service 12
BES12-Instanz	BES12-Instanz bezieht sich auf alle BES12-Komponenten, die auf einem Computer installiert sind, mit Ausnahme des BlackBerry Router, bei dem es sich um eine separat installierte optionale Komponente handelt. Eine BES12-Instanz wird auch manchmal als „Einheit“ bezeichnet.
Prozessübergreifendes BlackBerry-Protokoll	Das prozessübergreifende BlackBerry-Protokoll ist ein proprietäres Protokoll von BlackBerry, das den Sitzungsschlüssel generiert, mit dem BlackBerry Enterprise Solution-Komponenten, z. B. der BlackBerry Enterprise Server und das BlackBerry Mobile Voice System, auf äußerst sichere Weise miteinander kommunizieren können. Das prozessübergreifende BlackBerry-Protokoll generiert den Sitzungsschlüssel anhand des Kommunikationskennworts.
CA	Zertifizierungsstelle
Zertifikat	Ein Zertifikat ist ein digitales Dokument, das die Identität und den öffentlichen Schlüssel eines Zertifikatempfängers miteinander verknüpft. Für jedes Zertifikat ist ein entsprechender privater Schlüssel vorhanden, der getrennt gespeichert wird. Eine Zertifizierungsstelle signiert das Zertifikat und bescheinigt so seine Glaubwürdigkeit.
CRL	Certificate Revocation List (Zertifikatwiderrufliste)
DEP	Device Enrollment Program (Programm zur Geräteregistrierung)
DNS	Domain Name System (Domänennamensystem)
DPD	Dead Peer Detection
EAP	Extensible Authentication Protocol (erweiterbares Authentifizierungsprotokoll)
EAP-FAST	Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (Erweiterbares Authentifizierungsprotokoll – Flexible Authentifizierung über sichere Tunnel)
EAP-MS-CHAP	Extensible Authentication Protocol Microsoft® Challenge Handshake Authentication Protocol (erweiterbares Authentifizierungsprotokoll – Challenge Handshake Authentication-Protokoll von Microsoft®)
EAP-TLS	Extensible Authentication Protocol Transport Layer Security (erweiterbares Authentifizierungsprotokoll – Transportschichtsicherheit)

EMM	Enterprise Mobility Management
FQDN	Fully Qualified Domain Name (vollständiger Domänenname)
GTC	Generic Token Card
HMAC	Keyed-Hash Message Authentication Code (verschlüsselter Hash-Nachrichtenauthentifizierungscode)
HTTP	Hypertext Transfer Protocol (Hypertextübertragungsprotokoll)
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer (HTTP über SSL)
IKE	Internet Key Exchange
IMAP	Internet Message Access Protocol
IP	Internet Protocol (Internetprotokoll)
IPSec	Internet Protocol Security (Internetprotokollsicherheit)
IT-Richtlinie	Eine IT-Richtlinie besteht aus verschiedenen Regeln, die die Sicherheitsmerkmale und das Verhalten von Geräten steuern.
LAN	Local Area Network (lokales Netzwerk)
LDAP	Lightweight Directory Access Protocol (Anwendungsprotokoll)
MD5	Message-Digest Algorithm, Version 5 (Message-Digest-Algorithmus)
MDM	Mobile Geräteverwaltung (Mobile Device Management)
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol (Authentifizierungsprotokoll von Microsoft)
NAT	Network Address Translation
NTLM	NT LAN Manager (Authentifizierungsverfahren für Rechnernetze)
OCSP	Online Certificate Status Protocol (Internetprotokoll zur Statusabfrage)
PAC	Proxy Auto Configuration (Proxy-Autokonfiguration)
PFS	Perfekte Geheimhaltung bei der Weiterleitung
PKI	Public Key Infrastructure (Infrastruktur öffentlicher Schlüssel)
PMK	Pairwise Master Key
POP	Post Office Protocol
PRF	Pseudo-Random-Familie
PSK	Pre-Shared Key (vorinstallierter Schlüssel)
SCEP	Simple Certificate Enrollment-Protokoll
SHA	Secure Hash Algorithm (Sicherer Hash-Algorithmus)
S/MIME	Secure Multipurpose Internet Mail Extensions (Protokoll für den Austausch sicherer E-Mails über das Internet)

SNMP	Simple Network Management Protocol (einfaches Netzwerkverwaltungsprotokoll)
Bereich	Ein Bereich ist eine bestimmte Gerätezone, in der verschiedene Arten von Daten, Anwendungen und Netzwerkverbindungen getrennt und verwaltet werden können. Unterschiedliche Bereiche verfügen über unterschiedliche Regeln zur Datenspeicherung, für Anwendungsberechtigungen und Netzwerkroutings. Bereiche wurden bisher auch als Perimeter bezeichnet.
SSL	Secure Sockets Layer (Netzwerkprotokoll zur sicheren Übertragung von Daten)
Überwachte iOS-Geräte	Überwachte Geräte werden konfiguriert, damit die zusätzliche Steuerung von iOS-Gerätefunktionen ermöglicht wird. Um die Überwachung von iOS-Geräten im Besitz Ihrer Organisation zu aktivieren, können Sie den Apple Configurator oder das Device Enrollment-Programm verwenden.
TCP	Transmission Control Protocol (Übertragungssteuerungsprotokoll)
TIMA	ARM TrustZone based Integrity Measurement Architecture
TLS	Transport Layer Security (Netzwerkprotokoll zur sicheren Datenübertragung)
USB	Universal Serial Bus (serielles Bussystem zur Verbindung eines Computers mit externen Geräten)
VPN	Virtual Private Network (Virtuelles privates Netzwerk)
xAuth	Erweiterte Authentifizierung

Rechtliche Hinweise

© 2015 BlackBerry. Alle Rechte vorbehalten. BlackBerry® und zugehörige Marken, Namen und Logos sind Eigentum von BlackBerry Limited und sind in den USA und weiteren Ländern weltweit als Marken eingetragen und/oder werden dort als Marken verwendet.

Android, Google Chrome und Google Play sind Marken von Google Inc. Apple, App Store, Apple Configurator, iCloud und Safari sind Marken von Apple Inc. Aruba und VIA sind Marken von Aruba Networks, Inc. Bluetooth ist eine Marke von Bluetooth SIG. Check Point und VPN-1 sind Marken von Check Point Software Technologies Ltd. Cisco, Cisco AnyConnect, Cisco IOS und PIX sind Marken von Cisco Systems, Inc. und/oder seiner angegliederten Unternehmen in den USA und einigen anderen Ländern. F5 is a trademark of F5 Networks, Inc. HTC EVO ist eine Marke der HTC Corporation. IBM, Domino und Notizen sind eingetragene Marken der International Business Machines Corporation in vielen Ländern weltweit. iOS ist eine Marke von Cisco Systems, Inc. und/oder seiner angegliederten Unternehmen in den USA und einigen anderen Ländern. iOS® wird unter Lizenz von Apple Inc. verwendet. Juniper ist eine Marke von Juniper Networks, Inc. Kerberos ist eine Marke des Massachusetts Institute of Technology. Microsoft, Active Directory, ActiveSync, Windows und Windows Phone sind Marken oder eingetragene Marken der Microsoft Corporation in den USA und/oder anderen Ländern. OpenVPN ist eine Marke von OpenVPN Technologies, Inc. PGP ist eine Marke der PGP Corporation. RSA ist eine Marke von RSA Security. SonicWALL und Mobile Connect sind Marken von Dell, Inc. Symantec ist eine Marke oder eingetragene Marke der Symantec Corporation oder ihrer Tochtergesellschaften in den USA und anderen Ländern. T-Mobile ist eine Marke der Deutschen Telekom AG. Wi-Fi, WPA und WPA2 sind Marken der Wi-Fi Alliance. Entrust, Entrust IdentityGuard und Entrust Authority Administration Services sind Marken von Entrust, Inc. KNOX und Samsung KNOX sind Marken von Samsung Electronics Co., Ltd. Alle weiteren Marken sind Eigentum ihrer jeweiligen Inhaber.

Dieses Dokument und alle Dokumente, die per Verweis in dieses Dokument mit einbezogen werden, z. B. alle über die BlackBerry-Webseite erhältlichen Dokumente, werden ohne Mängelgewähr und je nach Verfügbarkeit bereitgestellt. Die entsprechenden Dokumente werden ohne ausdrückliche Billigung, Gewährleistung oder Garantie seitens BlackBerry Limited und seinen angegliederten Unternehmen („BlackBerry“) bereitgestellt. BlackBerry übernimmt keine Verantwortung für eventuelle typografische, technische oder anderweitige Ungenauigkeiten sowie für Fehler und Auslassungen in den genannten Dokumenten. Die BlackBerry-Technologie ist in dieser Dokumentation teilweise in verallgemeinerter Form beschrieben, um das Eigentum und die vertraulichen Informationen und/oder Geschäftsgeheimnisse von BlackBerry zu schützen. BlackBerry behält sich das Recht vor, die in diesem Dokument enthaltenen Informationen von Zeit zu Zeit zu ändern. BlackBerry ist jedoch nicht verpflichtet, die Benutzer über diese Änderungen, Updates, Verbesserungen oder Zusätze rechtzeitig bzw. überhaupt in Kenntnis zu setzen.

Diese Dokumentation enthält möglicherweise Verweise auf Informationsquellen, Hardware oder Software, Produkte oder Dienste, einschließlich Komponenten und Inhalte wie urheberrechtlich geschützte Inhalte und/oder Websites von Drittanbietern (nachfolgend "Drittprodukte und -dienste" genannt). BlackBerry hat keinen Einfluss auf und übernimmt keine Haftung für Drittprodukte und -dienste, dies gilt u. a. für Inhalt, Genauigkeit, Einhaltung der Urheberrechtsgesetze, Kompatibilität, Leistung, Zuverlässigkeit, Rechtmäßigkeit, Schicklichkeit, Links oder andere Aspekte der Drittprodukte und -dienste. Der Einschluss eines Verweises auf Drittprodukte und -dienste in dieser Dokumentation impliziert in keiner Weise eine besondere Empfehlung der Drittprodukte und -dienste oder des Drittanbieters durch BlackBerry.

SOFERN ES NICHT DURCH DAS IN IHREM RECHTSGEBIET GELTENDE RECHT AUSDRÜCKLICH UNTERSAGT IST, WERDEN HIERMIT SÄMTLICHE AUSDRÜCKLICHEN ODER KONKLUDENTEN BEDINGUNGEN, BILLIGUNGEN, GARANTIEN, ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN JEDER ART, EINSCHLIESSLICH, OHNE EINSCHRÄNKUNG, BEDINGUNGEN, BILLIGUNGEN, GARANTIEN, ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN HINSICHTLICH DER HALTBARKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER VERWENDUNGSZWECK, MARKTGÄNGIGKEIT, MARKTGÄNGIGEN QUALITÄT, NICHTVERLETZUNG VON RECHTEN DRITTER, ZUFRIEDENSTELLENDEN QUALITÄT ODER DES EIGENTUMSRECHTS ABGELEHNT. DIES GILT AUCH FÜR ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN, DIE SICH AUS EINEM GESETZ, EINER GEPFLOGENHEIT, USANCEN BZW. HANDELSGEPFLOGENHEITEN ERGEBEN ODER IM ZUSAMMENHANG MIT DER DOKUMENTATION ODER IHRER VERWENDUNG, DER LEISTUNG ODER MANGELNDEN LEISTUNG VON SOFTWARE, HARDWARE, DIENSTEN ODER DRITTANBIETER-PRODUKTEN UND -DIENSTEN STEHEN, AUF DIE HIER VERWIESEN WIRD. MÖGLICHERWEISE HABEN SIE ZUDEM ANDERE LANDESSPEZIFISCHE RECHTE. IN MANCHEN RECHTSGEBIETEN IST DER AUSSCHLUSS ODER DIE EINSCHRÄNKUNG KONKLUDENTER GEWÄHRLEISTUNGEN UND BEDINGUNGEN NICHT ZULÄSSIG. IN DEM GESETZLICH ZULÄSSIGEN UMFANG WERDEN SÄMTLICHE KONKLUDENTEN GEWÄHRLEISTUNGEN ODER BEDINGUNGEN IM ZUSAMMENHANG MIT DER DOKUMENTATION, DIE EINGESCHRÄNKT WERDEN KÖNNEN, SOFERN SIE NICHT WIE OBEN DARGELEGT AUSGESCHLOSSEN WERDEN KÖNNEN, HIERMIT AUF 90 TAGE AB DATUM DES ERWERBS DER DOKUMENTATION ODER DES ARTIKELS, AUF DEN SICH DIE FORDERUNG BEZIEHT, BESCHRÄNKT.

IN DEM DURCH DAS IN IHREM RECHTSGEBIET ANWENDBARE GESETZ MAXIMAL ZULÄSSIGEN AUSMASS HAFTET BLACKBERRY UNTER KEINEN UMSTÄNDEN FÜR SCHÄDEN JEGLICHER ART, DIE IM ZUSAMMENHANG MIT DIESER DOKUMENTATION ODER IHRER VERWENDUNG, DER LEISTUNG ODER NICHTLEISTUNG JEGLICHER SOFTWARE, HARDWARE, DIENSTE ODER DRITTPRODUKTE UND -DIENSTE, AUF DIE HIER BEZUG GENOMMEN WIRD, STEHEN, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE FOLGENDEN SCHÄDEN: DIREKTE, VERSCHÄRFTEN SCHADENERSATZ NACH SICH ZIEHENDE, BEILÄUFIG ENTSTANDENE, INDIREKTE, KONKRETE, STRAFE EINSCHLIESSENDE SCHÄDEN, FOLGESCHÄDEN ODER SCHÄDEN, FÜR DIE ANSPRUCH AUF KOMPENSATORISCHEN SCHADENERSATZ BESTEHT, SCHÄDEN WEGEN ENTGANGENEN GEWINNEN ODER EINKOMMEN, NICHTREALISIERUNG ERWARTETER EINSPARUNGEN, BETRIEBSUNTERBRECHUNGEN, VERLUSTES GESCHÄFTLICHER DATEN, ENTGANGENER GESCHÄFTSCHANCEN ODER BESCHÄDIGUNG BZW. VERLUSTES VON DATEN, DES UNVERMÖGENS, DATEN ZU ÜBERTRAGEN ODER ZU EMPFANGEN, PROBLEMEN IM ZUSAMMENHANG MIT ANWENDUNGEN, DIE IN VERBINDUNG MIT BLACKBERRY-PRODUKTEN UND -DIENSTEN VERWENDET WERDEN, KOSTEN VON AUSFALLZEITEN, NICHTVERWENDBARKEIT VON BLACKBERRY-PRODUKTEN UND -DIENSTEN ODER TEILEN DAVON BZW. VON AIRTIME-DIENSTEN, KOSTEN VON ERSATZGÜTERN, DECKUNG, EINRICHTUNGEN ODER DIENSTEN, KAPITAL- ODER ANDERE VERMÖGENSSCHÄDEN, UNABHÄNGIG DAVON, OB SCHÄDEN DIESER ART ABZUSEHEN ODER NICHT ABZUSEHEN WAREN, UND AUCH DANN, WENN BLACKBERRY AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE.

IN DEM DURCH DAS IN IHREM RECHTSGEBIET ANWENDBARE GESETZ MAXIMAL ZULÄSSIGEN AUSMASS ÜBERNIMMT BLACKBERRY KEINERLEI VERANTWORTUNG, VERPFLICHTUNG ODER HAFTUNG, SEI SIE VERTRAGLICHER, DELIKTRECHTLICHER ODER ANDERWEITIGER NATUR, EINSCHLIESSLICH DER HAFTUNG FÜR FAHRLÄSSIGKEIT UND DER DELIKTSHAFTUNG.

DIE IN DIESEM DOKUMENT GENANNTEN EINSCHRÄNKUNGEN, AUSSCHLÜSSE UND HAFTUNGSAUSSCHLÜSSE GELTEN: (A) UNGEACHTET DER VON IHNEN ANGEFÜHRTEN KLAGEGRÜNDE, FORDERUNGEN ODER KLAGEN, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF VERTRAGSBRUCH, FAHRLÄSSIGKEIT, ZIVILRECHTLICHER DELIKTE, DELIKTSHAFTUNG ODER SONSTIGE RECHTSTHEORIE UND SIND AUCH NACH EINEM WESENTLICHEN VERSTOSS BZW. EINEM FEHLENDEN GRUNDLEGENDEN ZWECK DIESER VEREINBARUNG ODER EINES DARIN ENTHALTENEN RECHTSBEHELFS WIRKSAM; UND GELTEN (B) FÜR BLACKBERRY UND DIE ZUGEHÖRIGEN UNTERNEHMEN, RECHTSNACHFOLGER, BEVOLLMÄCHTIGTEN, VERTRETER, LIEFERANTEN (EINSCHLIESSLICH AIRTIME-DIENSTANBIETERN), AUTORISIERTE BLACKBERRY-

DISTRIBUTOREN (EBENFALLS EINSCHLIESSLICH AIRTIME-DIENSTANBIETERN) UND DIE JEWEILIGEN FÜHRUNGSKRÄFTE, ANGESTELLTEN UND UNABHÄNGIGEN AUFTRAGNEHMER.

ZUSÄTZLICH ZU DEN OBEN GENANNTEN EINSCHRÄNKUNGEN UND AUSSCHLÜSSEN HAFTEN DIE FÜHRUNGSKRÄFTE, ANGESTELLTEN, VERTRETER, DISTRIBUTOREN, LIEFERANTEN, UNABHÄNGIGEN AUFTRAGNEHMER VON BLACKBERRY ODER BLACKBERRY ANGEHÖRENDEN UNTERNEHMEN IN KEINER WEISE IM ZUSAMMENHANG MIT DER DOKUMENTATION.

Bevor Sie Drittprodukte bzw. -dienste abonnieren, installieren oder verwenden, müssen Sie sicherstellen, dass Ihr Mobilfunkanbieter sich mit der Unterstützung aller zugehörigen Funktionen einverstanden erklärt hat. Einige Mobilfunkanbieter bieten möglicherweise keine Internet-Browsing-Funktion in Zusammenhang mit einem Abonnement für BlackBerry® Internet Service an. Erkundigen Sie sich bei Ihrem Dienstanbieter bezüglich Verfügbarkeit, Roaming-Vereinbarungen, Service-Plänen und Funktionen. Für die Installation oder Verwendung von Drittprodukten und -diensten mit den Produkten und Diensten von BlackBerry sind u. U. Patent-, Marken-, Urheberrechts- oder sonstige Lizenzen erforderlich, damit die Rechte Dritter nicht verletzt werden. Es liegt in Ihrer Verantwortung, zu entscheiden, ob Sie Drittprodukte und -dienste verwenden möchten, und festzustellen, ob hierfür Lizenzen erforderlich sind. Für den Erwerb etwaiger Lizenzen sind Sie verantwortlich. Installieren oder verwenden Sie Drittprodukte und -dienste erst nach dem Erwerb aller erforderlichen Lizenzen. Alle Drittprodukte und -dienste, die Sie mit Produkten und Diensten von BlackBerry erhalten, werden lediglich zu Ihrem Vorteil, ohne Mängelgewähr und ohne ausdrückliche oder stillschweigende Bedingung, Billigung, Garantie, Zusicherung oder Gewährleistung jedweder Art von BlackBerry bereitgestellt. BlackBerry übernimmt in diesem Zusammenhang keinerlei Haftung. Die Verwendung von Drittprodukten und -diensten unterliegt Ihrer Zustimmung zu den Bedingungen separater Lizenzen und anderer geltender Vereinbarungen mit Dritten, sofern sie nicht ausdrücklich von einer Lizenz oder anderen Vereinbarung mit BlackBerry behandelt wird.

Die Nutzungsbedingungen für BlackBerry-Produkte und -Dienste werden in einer entsprechenden separaten Lizenz oder anderen Vereinbarung mit BlackBerry dargelegt. KEINE DER IN DIESER DOKUMENTATION DARGELEGTEN BESTIMMUNGEN SETZEN IRGENDWELCHE AUSDRÜCKLICHEN SCHRIFTLICHEN VEREINBARUNGEN ODER GEWÄHRLEISTUNGEN VON BLACKBERRY FÜR TEILE VON BLACKBERRY-PRODUKTEN ODER -DIENSTEN AUSSER KRAFT.

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Veröffentlicht in Kanada